A MITEL
PRODUCT
GUIDE

Country Adaptations

Country Adaptations

Country Adaptations

Servicedokumentation
06/2022

A31003-H3100-S105-01-0020

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

Inhalt

1 Einleitung und wichtige Hinweise . . . 7
1.1 Zielgruppe dieses Buches . . . 7
1.2 Inhalt dieses Buches . . . 8
1.3 Hinweis zu Internet Explorer . . . 8
1.4 Verwendete Konventionen . . . 8

2 WBM des OpenScape 4000 SoftGates . . . 9
2.1 Hard- und Softwarevoraussetzungen . . . 9
2.1.1 Hardware . . . 9
2.1.2 Software . . . 9
2.1.3 Internet Explorer einstellen . . . 10
2.2 WBM starten und beenden . . . 12
2.2.1 Über OpenScape 4000 Assistant starten . . . 12
2.2.2 Über Web-Browser starten . . . 13
2.2.3 WBM-Sitzung beenden . . . 14
2.3 Benutzeroberfläche des WBMs . . . 15
2.3.1 Einteilung der Benutzeroberfläche . . . 15
2.3.2 Symbole im Steuerbereich des WBM-Fensters . . . 16
2.3.3 Dialogelemente . . . 17

3 Konfiguration . . . 19
3.1 Grundeinstellungen . . . 20
3.1.1 Gateway . . . 20
3.2 SIP Load Balancer . . . 21
3.2.1 Einstellungen . . . 23
3.2.2 Status . . . 24
3.3 Sicherheit . . . 26
3.3.1 MEK Verwaltung . . . 26
3.3.2 Sicherheitseinstellungen . . . 27
3.4 Ansagen/MoH . . . 29
3.4.1 Externe Ansagen . . . 29
3.4.2 Interne Ansagen . . . 30
3.5 WAN . . . 31
3.5.1 Einstellungen . . . 31
3.5.2 SPE . . . 32
3.5.2.1 Keycert importieren . . . 33
3.5.2.2 Keycert anzeigen . . . 34
3.5.2.3 Keycert löschen . . . 35
3.5.2.4 SPE Sicherheitseinstellungen . . . 35
3.6 LAN Interfaces . . . 37
3.6.1 Management Interface . . . 37
3.6.2 Signalling Survivability Interface . . . 38
3.6.3 XLink . . . 40
3.6.4 HFA Interface . . . 41
3.6.5 SIP Interface . . . 42
3.7 Diverse . . . 44
3.7.1 Fax-Parameter . . . 44
3.7.2 NGS . . . 45

3.7.3 QoS-Data-Collection . . . 46
3.8 Picture CLIP . . . 51
3.8.1 Einstellungen . . . 53
3.8.2 Test . . . 54
4 Wartung . . . 57
4.1 SW-Update . . . 58
4.1.1 SW-Version anzeigen . . . 58
4.1.2 LW-Update . . . 59
4.1.3 LW-Aktivierung . . . 59
4.1.4 OS-Update . . . 61
4.1.4.1 OS-Update Einstellungen . . . 61
4.1.4.2 OS-Update Aktionen . . . 62
4.2 Backup/Restore . . . 64
4.2.1 Export Konfiguration . . . 64
4.2.2 Export Sicherheitskonf . . . 65
4.2.3 Import Konfiguration . . . 65
4.2.4 Import Sicherheitskonf . . . 66
4.3 Logs . . . 68
4.3.1 Logs exportieren . . . 68
4.3.2 Logs löschen . . . 68
4.4 Trace . . . 70
4.4.1 Profile . . . 70
4.5 Secure Trace . . . 73
4.5.1 Zertifikat importieren . . . 74
4.5.2 Zertifikat anzeigen . . . 75
4.5.3 Status . . . 76
4.5.4 Trace starten . . . 76
4.5.5 Trace stoppen . . . 78
4.6 DLS Client . . . 79
4.6.1 DLS Einstellungen . . . 80
4.6.2 PIN Eingabe . . . 81
4.6.3 Bootstrapping zurücksetzen . . . 82
4.6.4 DLS kontaktieren . . . 82
4.6.4.1 DLSC Client-Zertifikate . . . 82
4.6.4.2 1. DLSC Client-Zertifikat . . . 83
4.6.4.3 DLSC CA-Zertifikate . . . 83
4.6.4.4 „1. CA-Zertifikat“, „2. CA-Zertifikat“ . . . 84
4.7 Diagnose . . . 85
4.7.1 Diagnose-Funktionen . . . 85
4.7.1.1 Interne LAN Capture-Kontrolle . . . 85
4.7.1.2 Thread-Profiling . . . 86
4.7.1.3 Heap-Überwachung . . . 87
4.7.2 Diagnose-Dateien . . . 87
4.8 Status-Information . . . 89
4.8.1 System-Information . . . 89
4.8.1.1 Thread Zustände anzeigen . . . 89
4.8.1.2 Periphere Baugruppen . . . 90
4.8.1.3 OpenScape Access Module . . . 91
4.8.1.4 OpenScape Access Clocking . . . 94
4.8.1.5 AP Emergency . . . 95
4.8.2 SoftGate-Verbindungskontrolle . . . 95

4.8.2.1 IPDA Verbindungen anzeigen 96
4.8.2.2 IPDA DMC Verbindungen anzeigen 96
4.8.2.3 Alle Verbindungen anzeigen 97
4.8.3 H323-Status 97
4.8.3.1 H323 Endpunkte 98
4.8.4 HFA WAN Clients 99
4.8.4.1 Status 99
4.8.4.2 Logon Versuche 99
4.9 Reboot / Shutdown OS 100
4.9.1 Reboot / Shutdown OS 100
5 Hilfe 101
6 Abmelden 103

1 Einleitung und wichtige Hinweise

OpenScape 4000 SoftGate und vHG 3575

OpenScape 4000 SoftGate ist eine IP-Telefonie-Applikation für den Anschluss von HFA- und SIP-basierten Telefonen, z.B. für die Telefonfamilien OpenStage HFA und OpenStage SIP. Sie ermöglicht IP-basierte Kommunikation im gesamten Unternehmen einschließlich kleiner Außenstellen. Der Anschluss an das öffentliche Telefonnetz wird durch SIP-Trunking (SIP-Q oder native SIP) ermöglicht.

Die vHG 3575 (virtuelle HG 3575 = virtuelle NCUI) ist im OpenScape 4000 SoftGate die zentrale Steuerung für die IPDA (IP Distributed Architecture).

Themen in diesem Kapitel

Abschnitt 1.1, “Zielgruppe dieses Buches”
Abschnitt 1.2, “Inhalt dieses Buches”
Abschnitt 1.3, “Hinweis zu Internet Explorer”
Abschnitt 1.4, “Verwendete Konventionen”

1.1 Zielgruppe dieses Buches

Dieses Buch ist für Mitarbeiter gedacht, die für die Administration der vHG 3575 und OpenScape 4000 SoftGate verantwortlich sind. Sie müssen bereits Erfahrung in der Administration von LANs haben und insbesondere über fundierte Kenntnisse in den folgenden Bereichen verfügen:

- Hardware für die Datenkommunikation
- OpenScape 4000 V8
- Konzepte und Begriffe für Weitbereichsnetze (WAN)
- Konzepte und Begriffe für lokale Netze (LAN)
- Konzepte und Begriffe für das Internet

Sie sollten für vHG 3575 und OpenScape 4000 SoftGate eine Einweisung in den folgenden Bereichen erhalten haben:

- Installation und Inbetriebnahme
- Konfiguration der VoIP-Funktionen
- Einrichtung und Konfiguration der Datenkommunikationsparameter

1.2 Inhalt dieses Buches

Dieses Buch beschreibt das WBM (Web-Based Management) der vHG 3575 für OpenScape 4000 SoftGate. Dazu gehören die allgemeine Bedienung des WBMs, Beschreibungen der einzelnen Module für die Administration der vHG 3575 und auch, wie bei der Administration vorzugehen ist.

1.3 Hinweis zu Internet Explorer

WICHTIG: Wenn Sie Änderungen an den Internet Explorer Sicherheitseinstellungen für eine WBM-Seite vorgenommen haben (z.B.: die Seite den Trusted Sites hinzugefügt), so wird empfohlen, den Browser neu zu starten, damit die neuen Einstellungen korrekt verwendet werden.

1.4 Verwendete Konventionen

In diesem Buch werden die folgenden typographischen Konventionen verwendet:

Konvention	Beispiel
`Courier`	Eingabe und Ausgabe Beispiel: `LOCAL` als Dateiname eingeben `Befehl nicht gefunden`
Kursiv	Variable Beispiel: *Name* kann bis zu acht Zeichen lang sein
Kursiv	Elemente der Benutzeroberfläche Beispiel: Klicken Sie auf die Schaltfläche *OK*.
Abschnitt 1.4, “Verwendete Konventionen”	Querverweis
Konfiguration	Elemente der Benutzeroberfläche als Querverweis
Fett	Besondere Hervorhebung Beispiel: Dieser Name darf **nicht** gelöscht werden
`<Courier>`	Tastenkombinationen Beispiel: `<STRG>+<ALT>+<ESC>`
>	Menüfolge Beispiel: *WBM* **>** *Konfiguration*
WICHTIG:	Kennzeichnet Situationen, die Sachschäden und/oder Datenverlust zur Folge haben können.
HINWEIS:	Kennzeichnet hilfreiche Hinweise.

2 WBM des OpenScape 4000 SoftGates

WBM

Das WBM ist die Administrationsoberfläche der vHG 3575 für OpenScape 4000 SoftGate (virtuelle HG 3575 = virtuelle NCUI). Sofern der Root-Administrator das WBM aktiviert hat, steht es über jede TCP/IP-Verbindung zur Verfügung, sowohl über das LAN als auch das WAN.

Jeder PC mit TCP/IP-gestützter Netzwerkverbindung, auf dem ein kompatibler Web-Browser läuft, kann nach erfolgreicher Anmeldung am OpenScape 4000 Assistant auf das WBM zugreifen. Das WBM der vHG 3575 verfügt über einen integrierten Web-Server, so dass es über eine HTTP-URL (bei aktiviertem SSL eine HTTPS-URL) aufrufbar ist.

Die Bedienoberfläche des WBMs ist in den Sprachen Deutsch und Englisch verfügbar. Die Sprachumschaltung geschieht über die Spracheinstellung des Web-Browsers.

Themen in diesem Kapitel

Abschnitt 2.1, “Hard- und Softwarevoraussetzungen”
Abschnitt 2.2, “WBM starten und beenden”
Abschnitt 2.3, “Benutzeroberfläche des WBMs”

2.1 Hard- und Softwarevoraussetzungen

2.1.1 Hardware

Für das WBM benötigen Sie einen Administrations-PC mit folgender Mindestausstattung:

- 128 MB Hauptspeicher (RAM)
- Prozessor-Taktrate 400 MHz

2.1.2 Software

Das WBM der vHG 3575 besteht aus HTML/XSL-Seiten mit Frames. Sein Einsatz erfordert:

- Windows NT 4.0, 2000, XP, Vista oder Windows 7
- Microsoft Internet Explorer 6, 7, 8

  Im Internet Explorer sind die unten beschriebenen Einstellungen vorzunehmen, siehe Abschnitt 2.1.3, “Internet Explorer einstellen”.

Andere Browser, die Frames, Java und JavaScript unterstützen, sind möglicherweise ebenfalls mit dem WBM kompatibel. Browser, die keine Frames unterstützen, können nicht mit dem WBM verwendet werden.

WICHTIG: Wenn auf dem Administrations-PC ein DNS-Server eingerichtet wurde, der aber nicht erreichbar ist, führt dies bei der WBM-Oberfläche zu erheblichen Geschwindigkeitseinbußen. Sollte dies bei Ihnen der Fall sein, überprüfen Sie in den Netzwerkeinstellungen des Administrations-PCs die eingestellten DNS-Server. Entfernen Sie nicht erreichbare DNS-Server, oder tragen Sie erreichbare Server ein.

2.1.3 Internet Explorer einstellen

Im Internet Explorer sind die folgenden Einstellungen vorzunehmen:

ActiveX aktivieren (nur für Internet Explorer 6)

Extras **>** *Internetoptionen* **>** Registerkarte *Sicherheit* **>** Webinhaltszone *Lokales Intranet* **>** Schaltfläche *Stufe anpassen* **>***ActiveX-Steuerelemente und Plugins* **>** *ActiveX-Steuerelemente ausführen, die für Scripting sicher sind* **>** *Aktivieren*

Kompatibilitätsansicht aktivieren (bei Internet Explorer 8)

Falls im Internet Explorer 8 Darstellungsprobleme auftreten, wird empfohlen, die Kompatibilitätsansicht zu aktivieren:

1. WBM im Internet Explorer 8 starten.
2. Kompatibilitätsansicht aktivieren:
   a) *Extras* **>** *Einstellungen der Kompatibilitätsansicht*. Das Fenster *Einstellungen der Kompatibilitätsansicht* wird geöffnet. Im Eingabefeld *Folgende Websites hinzufügen* steht bereits die IP-Adresse des WBMs.
   b) Auf *Hinzufügen* klicken. Die IP-Adresse des WBMs wird zur Liste *Zur Kompatibilitätsansicht hinzugefügte Websites* hinzugefügt.
   c) Auf *Schließen* klicken.

Java aktivieren

Extras **>** *Internetoptionen* **>** Registerkarte *Sicherheit* **>** Webinhaltszone *Lokales Intranet* **>** Schaltfläche *Stufe anpassen* **>** *Scripting* **>** *Active Scripting* **>** *Aktivieren*

Temporäre Internet-Dateien löschen

Extras **>** *Internetoptionen* **>** *Erweitert* **>** *Sicherheit* **>** Aktivieren: *Leeren des Ordners "Temporary Internet Files" beim Schließen des Browsers*

Proxyserver umgehen

Die Verbindung des Administrations-PC zur vHG 3575 darf nicht über einen Proxyserver erfolgen.

Extras **>** *Internetoptionen* **>** Registerkarte *Verbindungen* **>** *LAN-Einstellungen* **>** Schaltfläche *Einstellungen* **>** *Proxyserver* **>** Aktivieren: *Proxyserver für lokale Adressen umgehen*

Download von Dateien ermöglichen

- Entweder für alle URLs:

  Extras **>** *Internetoptionen* **>** Registerkarte *Sicherheit* **>** Webinhaltszone *Lokales Intranet* **>** Schaltfläche *Stufe anpassen* **>** *Download* **>** *Dateidownload* **>** *Aktivieren*

- Oder nur für die URL des WBMs der vHG 3575:

  1. *Extras* **>** *Internetoptionen* **>** Registerkarte *Sicherheit* **>** Webinhaltszone *Vertrauenswürdige Sites* **>** Schaltfläche *Sites* **>** URL des WBMs eingeben in *Diese Website zur Zone hinzufügen* **>** Schaltfläche *Hinzufügen*, Aktivieren: Kontrollkästchen *Für Sites dieser Zone ist eine Serverüberprüfung (https:) erforderlich*
  2. *Extras* **>** *Internetoptionen* **>** Registerkarte *Sicherheit* **>** Webinhaltszone *Vertrauenswürdige Sites* **>** Schaltfläche *Stufe anpassen* **>** *Download* **>** *Dateidownload* **>** *Aktivieren*

Nachdem alle Einstellungen vorgenommen wurden, ist der Internet Explorer zu schließen und neu zu starten.

2.2 WBM starten und beenden

Zugangsmöglichkeiten

Zum Starten des WBMs der vHG 3575 für OpenScape 4000 SoftGate gibt es zwei Möglichkeiten. Zum einen über OpenScape 4000 Assistant, zum anderen direkt über einen Web-Browser und die URL des WBMs. Der Zugang über OpenScape 4000 Assistant ist die am häufigsten benutzte Möglichkeit.

Themen in diesem Abschnitt

Abschnitt 2.2.1, “Über OpenScape 4000 Assistant starten”
Abschnitt 2.2.2, “Über Web-Browser starten”
Abschnitt 2.2.3, “WBM-Sitzung beenden”

2.2.1 Über OpenScape 4000 Assistant starten

Führen Sie zum Starten der WBM-Sitzung die folgenden Schritte durch:

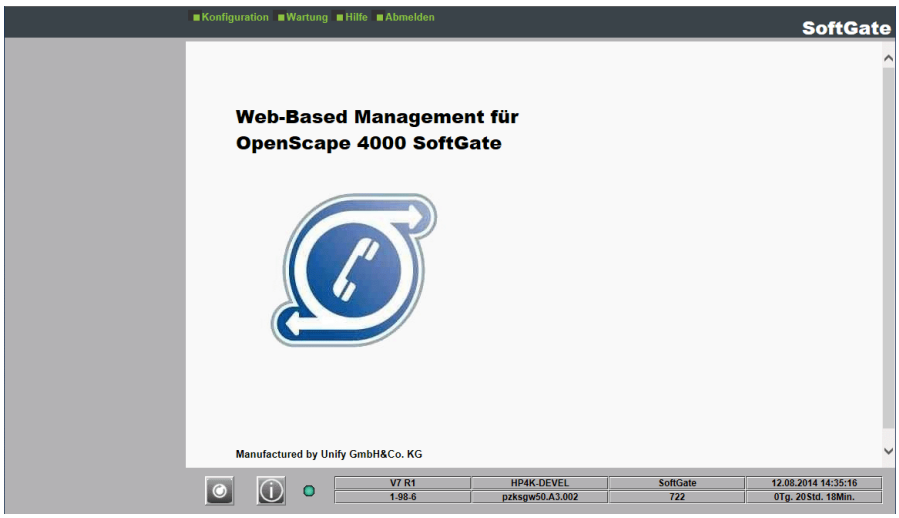
1. Melden Sie sich mit Ihrem Benutzernamen und Ihrem Kennwort am OpenScape 4000 Assistant an.
2. Wählen Sie in der Baumstruktur *OpenScape 4000 Assistant* **>** *Experten-modus* **>** *Gateway Dashboard*. Das Fenster *Gateway Dashboard* mit den vorhandenen Baugruppen wird angezeigt.
3. Klicken Sie in der Zeile der gewünschten Baugruppe vHG 3575 (z. B. SoftGate) in der Spalte *Remote-Zugang* auf *[WBM] [N/A]*. Die IP-Adresse der entsprechenden Baugruppe muss Ihnen bekannt sein.

   Der Web-Server des WBMs wird kontaktiert. Da er ausschließlich mit HTTPS (gesicherter Datenübertragung) arbeitet, sendet der Server ein Zertifikat.

   HINWEIS: Im Internet Explorer 8 kann die Meldung erscheinen, dass ein Problem mit dem Sicherheitszertifikat der Website besteht. Klicken Sie in diesem Fall auf *Laden dieser Website fortsetzen*.

   ---

4. Bestätigen Sie den Browser-Dialog mit den Zertifikatsinformationen. Die Startseite des WBMs der vHG 3575 wird angezeigt:



5. Überprüfen Sie, ob Sie sich im WBMs der vHG 3575 (z.B. SoftGate) befinden.
6. In den Modulen *Konfiguration* und *Wartung* können Sie jetzt die vHG 3575 administrieren.

2.2.2 Über Web-Browser starten

Benutzerkennung

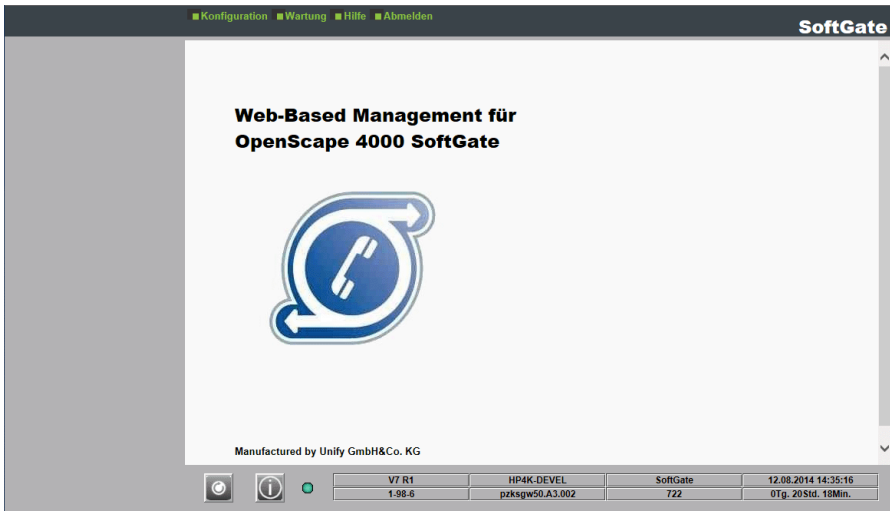
Für das WBM steht Ihnen die Benutzerkennung „Administrator“ zur Verfügung. Diese Kennung bietet Ihnen Zugang zu den Konfigurationseinstellungen.

Der Standard-Benutzername lautet **TRM** und das Standard-Kennwort **HICOM** (wie im AMO STMIB konfiguriert). Diese Standard-Daten können von Ihnen im AMO STMIB geändert werden.

WBM-Sitzung starten

Führen Sie zum Starten der WBM-Sitzung die folgenden Schritte durch:

1. Öffnen Sie Ihren Web-Browser.
2. Geben Sie in die Adresszeile des Web-Browsers die URL des WBMs der vHG 3575 ein, d.h. im Format *https://999.999.999.999*. Der Webserver des WBMs wird kontaktiert. Da er ausschließlich mit HTTPS (gesicherter Datenübertragung) arbeitet, sendet der Server ein Zertifikat.
3. Bestätigen Sie den Browser-Dialog mit den Zertifikatsinformationen. Der Anmeldedialog des WBMs der vHG 3575 wird angezeigt.
4. Geben Sie den Benutzernamen und das Kennwort ein. Klicken Sie auf die Schaltfläche *Login*. Die Startseite des WBMs der vHG 3575 wird angezeigt:



5. In den Modulen *Konfiguration* und *Wartung* können Sie jetzt die vHG 3575 administrieren.

2.2.3 WBM-Sitzung beenden

Führen Sie zum Beenden der WBM-Sitzung die folgenden Schritte durch:

1. Klicken Sie auf das Modul Abmelden. Die Verbindung zum WBM die vHG 3575 wird beendet und die WBM-Sitzung wird geschlossen.

Erläuterungen zum Beenden der WBM-Sitzung finden Sie im Kapitel 6, „Abmelden“.

2.3 Benutzeroberfläche des WBMs

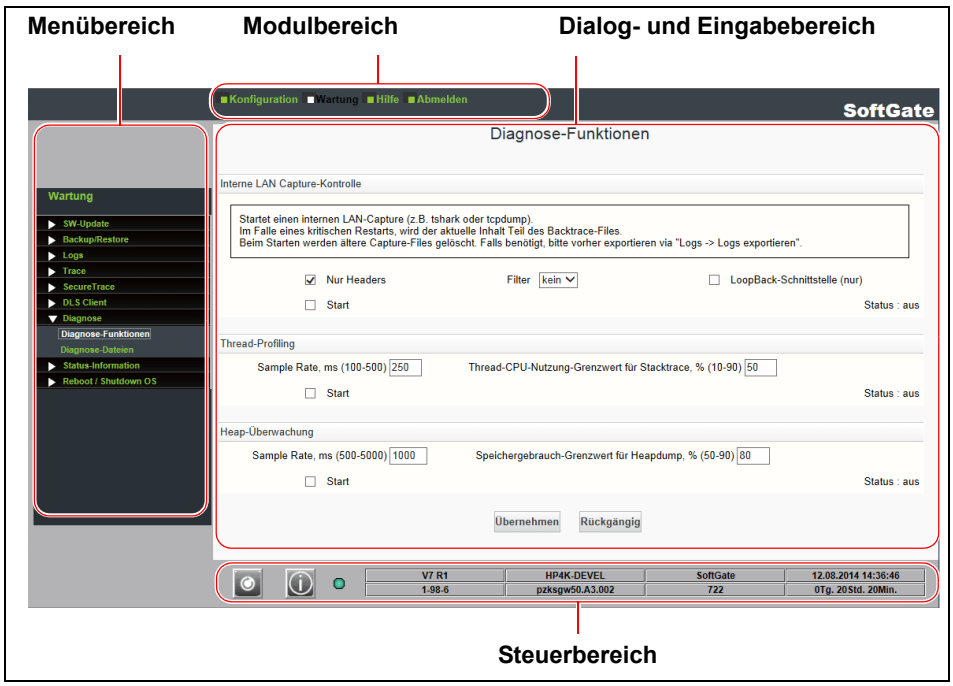
Dieser Abschnitt erklärt den grundsätzlichen Aufbau der Benutzeroberfläche, nennt die einzelnen Bedienelemente und beschreibt deren Benutzung.

Themen in diesem Abschnitt

Abschnitt 2.3.1, “Einteilung der Benutzeroberfläche”
Abschnitt 2.3.2, “Symbole im Steuerbereich des WBM-Fensters”
Abschnitt 2.3.3, “Dialogelemente”

2.3.1 Einteilung der Benutzeroberfläche

Die Benutzeroberfläche des WBMs lässt sich in die folgenden Bereiche einteilen:



Menübereich

Dieser Bereich wird für die Navigation innerhalb eines Moduls verwendet. Welche Menüeinträge dort angezeigt werden, hängt vom gewählten Modul ab.

Modulbereich

Dieser Bereich zeigt die zur Verfügung stehenden Module an. Die Module sind: *Konfiguration*, *Wartung*, *Hilfe* und *Abmelden*. Durch Klicken auf den Namen des Moduls erscheinen im Menübereich die zugehörigen Menüeinträge.

Dialog- und Eingabebereich

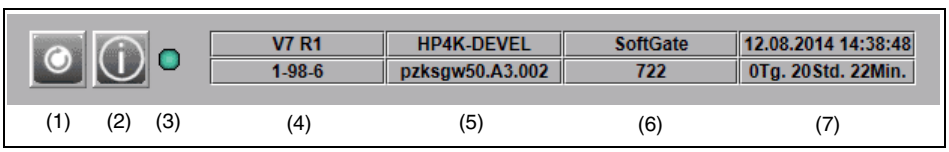
In diesem Bereich erscheinen nach Auswählen des Moduls und des Menüeintrages die jeweiligen Einstellungsdialoge.

Steuerbereich

Am unteren Rand finden Sie einige ständig angezeigte Statusinformationen. Zur Bedeutung der Symbole siehe Abschnitt 2.3.2, “Symbole im Steuerbereich des WBM-Fensters”.

2.3.2 Symbole im Steuerbereich des WBM-Fensters

Der Steuerbereich stellt ständig Steuer- und Statusinformationen bereit. Die Abbildung unten zeigt ein Beispiel:



Es gibt folgende Steuersymbole:

Reset-Symbol (1)

Dieses Symbol kann folgende Zustände annehmen:

Weiß/grau: Die Dateneingabe ist gesperrt. Der Benutzer kann Daten lesen aber keine Einträge ändern.

Weiß/schwarz: Die Dateneingabe ist aktiviert. Durch das Klicken auf dieses Symbol wird ein Neustart der vHG 3575 ausgelöst.

Informations-Symbol (2)

Nach dem Klicken auf dieses Symbol werden Informationen zum Betriebsstatus von OpenScape 4000 SoftGate angezeigt, z. B. in Betrieb/Nicht in Betrieb, Hostname, Ort, Softwareversion.

Aktivitäts-Symbol (3)

Das Symbol leuchtet grün, wenn eine Verbindung zum Webserver des WBMs besteht. Wenn keine Verbindung besteht, blinkt das Symbol rot.

Außerdem werden folgende Statusinformationen angezeigt:

- Zustandsinformation der ITIL-Version (4),
- Zugangskategorie des Benutzers und Systemversion (5),
- Name der Baugruppe und Aufstellungsort (6),
- Systemdatum und -uhrzeit sowie Zeit seit dem letzten Neustart (7).

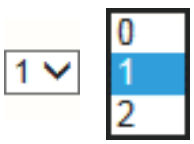
2.3.3 Dialogelemente

Im WBM kommen die folgenden Dialogelemente vor:

Eingabefelder

Eingaben von numerischen oder alphanumerischen Werten. Vor, hinter oder über dem Feld steht die zugehörige Feldbeschriftung. Bei Passwortfeldern werden zur Sicherheit nur einheitliche Symbole wie Sternchen für jedes eingegebene Zeichen angezeigt. Nicht auf der Tastatur verfügbare Zeichen können unter Microsoft Windows z. B. über die Zeichentabelle eingefügt werden.

Auswahlfelder



(im nebenstehenden Bild link geschlosen, rechts geöffnet) Auf den Pfeil klicken, um die Liste zu öffnen oder zu schließen. Den gewünschten Eintrag mit der Maus anklicken.

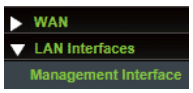
Kontrollkästchen

(im nebenstehenden Bild oben ausgeschaltet, unten eingeschaltet): Vor, hinter oder über dem Feld steht die zugehörige Feldbeschriftung. Anklicken, um die entsprechende Option ein- oder auszuschalten. Es können mehrere Kontrollkästchen aktiviert sein.

Radio-Buttons

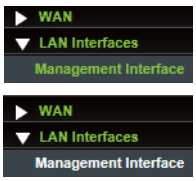
(im nebenstehenden Bild oben ausgeschaltet, unten eingeschaltet): In einer zusammengehörigen Gruppe solcher Elemente ist stets eines eingeschaltet und alle anderen ausgeschaltet. Vor, hinter oder über dem Feld steht die zugehörige Feldbeschriftung. Anklicken, um die entsprechende Funktion einzuschalten.

Dreiecke



(im nebenstehenden Bild oben: Menü geschlossen, unten: Menü geöffnet): Im Menübereich kann durch Klicken auf ein Dreieck ein Menü geöffnet oder geschlossen werden. Das Öffnen von mehreren Menüs ist möglich.

Menüpunkte



(im nebenstehenden Bild oben: Menüpunkt nicht aktiv, unten: Menüpunkt aktiv): Durch Klicken auf einen Menüpunkt wird der dazugehörige Dialog angezeigt. Ein nicht aktiver Menüpunkt ist grün, ein aktiver Menüpunkt ist weiß.

Schaltflächen

Bei Anklicken wird die Aktion ausgeführt, die als Text auf der Schaltfläche steht. Die Texte sind selbsterklärend, wie z. B. *Rückgängig* oder *Übernehmen*.

Sortierreihenfolge

In einer Tabelle kann durch Anklicken des Dreiecks neben der Überschrift in einem Tabellenkopf die Sortierreihenfolge in der darunterliegenden Spalte geändert werden, z. B. alphabetisch aufsteigend oder absteigend.

3 Konfiguration

WBM-Pfad

WBM **>** *Konfiguration*

Das Modul *Konfiguration* wird geöffnet.

Das Modul *Konfiguration* dient zum Festlegen der Grundeinstellungen sowie zum Konfigurieren der folgenden Einstellungen des OpenScape 4000 SoftGates:

Auswahlmöglichkeiten im Modul *Konfiguration*

Grundeinstellungen
SIP Load Balancer
Sicherheit
Ansagen/MoH
WAN
LAN Interfaces
Diverse
Picture CLIP

3.1 Grundeinstellungen

Im Menü *Grundeinstellungen* können grundsätzliche Daten der vHG 3575 eingegeben werden.

WBM-Pfad

WBM **>** *Konfiguration* **>** *Grundeinstellungen*

Das Menü *Grundeinstellungen* wird geöffnet:.

Menü *Grundeinstellungen*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

Gateway

3.1.1 Gateway

WBM-Pfad

WBM **>** *Konfiguration* **>** *Grundeinstellungen* **>** *Gateway*

Der Dialog *Gateway-Eigenschaften* wird angezeigt. In diesem Dialog können grundsätzliche Daten eingegeben werden.

Eingabefelder

In diesem Dialog gibt es die folgenden Eingabefelder:

- *System-Name*: In dieses Feld ist der Name der vHG 3575 einzugeben, z.B. wenn an einem OpenScape 4000 SoftGate mehrere vHG 3575 betrieben werden.
- *Gateway-Standort*: In diesem Feld wird der Standort der vHG 3575 angezeigt.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert.
- *Rückgängig:* Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt.

3.2 SIP Load Balancer

RQ00030342

WBM-Pfad

WBM **>** *Konfiguration* **>** *SIP Load Balancer*

Das Menü *SIP Load Balancer* wird geöffnet.

Menü *SIP Load Balancer*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

Einstellungen
Status

Leistungsmerkmalbeschreibung

SIP-Load-Balancing wird zur Lastverteilung des SIP-bezogenen Datenverkehrs im IP-Netzwerk eingesetzt. Damit wird die Leistung der beteiligten SIP-Server skaliert, eine Überlastung der Server vermieden und eine hohe Verfügbarkeit der SIP-Dienste erreicht.

Load Balancing dient dazu, Rufe von einem Provideranschluss, einer OpenScape UC oder OpenScape Xpressions auf mehrere Gateways zu verteilen, z.B. wenn der Anschluss mehr als die maximalen Kanäle eines Gateways hat. Bei einem Provideranschluss kann nur eine Ziel-IP-Adresse konfiguriert werden, so dass ohne Load Balancing pro Gateway ein Providerderanschluss vorhanden sein müsste.

Mit Hilfe der pro Gateway konfigurierbaren Routing-Nummern (z.B. der Ortsvorwahl) können Rufe auch anhand ihrer Rufnummer gezielt von einem Anschluss an bestimmte auch örtlich verteilte Gatewaygruppen, bzw. OpenScape-4000-Anlagen, gesendet werden. Innerhalb einer Gruppe werden die Rufe an das Gateway mit den meisten freien Kanälen gesendet.

SIP-Load-Balancing kann für jedes SIP-Gateway (HG 3500 oder vHG 3500 SIP) im Netzwerk aktiviert werden. Ist das Leistungsmerkmal korrekt aktiviert, registrieren sich die teilnehmenden Gateways automatisch am SIP Load Balancing Server.

SIP Load Balancing wird auch mit mehreren OpenScape UC Media Servern freigegeben. Diese können sich nicht automatisch beim SIP Load Balancing Server registrieren, deshalb müssen diese manuell im OpenScape 4000 SoftGate WBM konfiguriert werden.

Serviceinformationen für OpenSIPS Load Balancer

Der OpenSIPS Load Balancer ist Teil des OpenScape 4000 SoftGate Softwarepaketes und wird mit jedem OpenScape 4000 SoftGate installiert. Er läuft auf dem OpenScape 4000 SoftGate hat aber eine eigene (von dem OpenScape 4000 SoftGate verschiedene) IP-Adresse. Die IP-Adresse wird während der Installation eingerichtet.

Mit Hilfe seiner konfigurierten IP-Adressen holt sich der Load Balancer automatisch seinen eventuell vorhandenen DNS-Server-Namen vom DNS-Server.

Das Leistungsmerkmal Load Balancing ist per default ausgeschaltet und muss über das WBM des OpenScape 4000 SoftGates und das WBM jedes teilnehmenden Gateways eingeschaltet werden.

Leistungsmerkmale:

- "Load Balancing" für Inbound native SIP-Verbindungen zu virtuellen HG 3500 Gateways (OpenScape 4000 SoftGate) und den auf dem Betriebssystem vxWorks basierten HG 3500 Gateways (IPDA) (z.B. bei SIP Provider oder OpenScape UC Anbindung).
- Unterstützt native SIP Trunks ohne Registrierung.
- Virtuelle HG 3500 Gateways unterschiedlicher OpenScape 4000 SoftGates und HG 3500 Gateways in unterschiedlichen Access Points werden unterstützt.
- Error Logging / Tracing mit OpenSIPS.
- Sicherheit in der Datenübertragung zwischen den vHG 3500/HG 3500 und OpenSIPS (über authentifiziertes https).
- Failover Mechanismen für Inbound-Verbindungen, die vom Gateway auf Grund von Fehlermeldungen abgewiesen wurden.
- Status Monitoring der konfigurierten Gateways über den OpenSIPS Load Balancer.
- Load Balancing für verschiedene Gruppen von Gateways.

Voraussetzungen:

- Im Netzverbund muss ein OpenScape 4000 SoftGate vorhanden sein.
- SIP-Load-Balancing kann nur aktiviert werden, wenn die Verwendung von SIP-Trunking-Profilen aktiviert ist:
- Damit SIP-Load-Balancing funktionieren kann, muss sichergestellt werden, dass die (Outbound)-Proxy-Einstellungen im SIP-Trunking-Profil korrekt konfiguriert sind.

Einschränkungen:

Das Leistungsmerkmal “SIP Load Balancing” kann nur bei einem “Standalone SoftGate” Deployment verwendet werden. Es steht also zum Beispiel für “Survivable SoftGate” nicht zur Verfügung.

Generierung:

WICHTIG: Eine Generierung über AMOs ist nicht möglich.

3.2.1 Einstellungen

Der SIP-Load-Balance Server wird über das WBM des OpenScape 4000 SoftGates aktiviert. Dazu muss die IP-Adresse des Load Balancers und die Netzwerkmaske eingegeben werden.

Nach jeder Aktivierung/Deaktivierung oder Änderung der IP-Adresse des Load Balancers ist ein Restart des OpenScape 4000 SoftGates notwendig.

WBM-Pfad

WBM **>** *Konfiguration* **>** *SIP Load Balancer* **>** *Einstellungen*

Der Dialog *SIP Load Balancer Einstellungen* wird geöffnet.

Eingabefelder/Kontrollkästchen

Im Dialog *SIP Load Balancer Einstellungen* ist einzustellen:

- *IP Adresse [IPv4]*: In dieses Eingabefeld ist die IP-Adresse des SIP-Load-Balance-Servers im IPv4-Format einzugeben.
- *Netzwerkmaske [IPv4]*: In dieses Eingabefeld ist die Netzwerkmaske des Sub-Netzes im IPv4-Format einzugeben, in dem sich SIP-Load-Balance Server befindet.
- *Default Gateway [IPv4]*: In dieses Eingabefeld ist die IP-Adresse des Default-Gateways im IPv4-Format einzugeben.
- *VLAN Tagging verwenden*: Aktivierbar/deaktivierbar. Mit IEEE802.1p/q wird ermöglicht, dass sich mehrere virtuelle LANs ein gemeinsames physikalisches Netz teilen. Das virtuelle LAN ist paketbasiert, im Gegensatz zu älteren portbasierten LANs. Im Datenbereich des Ethernet-Pakets befindet sich ein Tag, das definiert, zu welchem VLAN das Ethernet-Paket gehört und welche Priorität das Datenpaket hat.
- *VLAN ID*: Jedem VLAN wird eine eindeutige Nummer zugeordnet, die VLAN-ID. Alle Geräte, welche dieselbe VLAN-ID haben, können miteinander kommunizieren.

- *Aktivieren*: Aktivierbar/deaktivierbar. Die geänderten Einstellungen dieses Dialoges aktivieren.

WICHTIG: Damit alle Konfigurationsänderungen wirksam werden, muss OpenScape 4000 SoftGate bzw. OpenScape Access 500i/a bzw. neu gestartet werden.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen sind OpenScape Access 500i/a bzw. OpenScape 4000 SoftGate neu zu starten.
- *Rückgängig:* Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt.

3.2.2 Status

Es werden die konfigurierten Gateways für das SIP Load Balancing angezeigt.

WBM-Pfad

WBM **>** *Konfiguration* **>** *SIP Load Balancer* **>** *Status*

Die Tabelle *SIP Load Balancer Status* wird geöffnet.

Spalten

In der Tabelle *SIP Load Balancer Status* gibt es folgende Spalten:

- *PBX*: Lage des Gateways bei OpenScape 4000
- *LTU*: Line Trunk Unit. Shelf 17 - 99 sind über IPDA mit dem Prozessor verbunden.
- *Slot*: Einbauteilung des OpenScape 4000 Gateways
- *Gateway IPv4 Address*: IP-Adresse des Gateways im IPv4-Format
- *IPv4 Port*: SIP-Port 5060 wird benutzt für nicht verschlüsselte Signalisierungsdaten.
- *IPv4 TLS Port*: SIP-Port 5061 wird benutzt für mit TLS (Transport Layer Security) verschlüsselte Signalisierungsdaten.
- *Gateway IPv6 Address*: IP-Adresse des Gateways im IPv6-Format
- *IPv6 Port*: SIP-Port 5060 wird benutzt für nicht verschlüsselte Signalisierungsdaten.

- *IPv6 TLS Port*: SIP-Port 5061 wird benutzt für mit TLS (Transport Layer Security) verschlüsselte Signalisierungsdaten.
- *Routing Number*: Einwahlnummern (z.B. +4982700332200 für "1" und +4982700332201 für "11")
- *Max Number of B-Channels*: Es sollte die maximal mögliche Anzahl paralleler B-Kanäle verwendet werden.
- *Load*: Auslastung des Gateways
- *Enabled*: Anzeige, ob der Gateway erreichbar ist.

Schaltflächen

In der Tabelle *SIP Load Balancer Status* gibt es folgende Schaltflächen:

- *Delete Rule*: Regel für den Gateway löschen.
- Add Rule: Regel für einen Gateway erstellen.

3.3 Sicherheit

Im Menü Sicherheit können Sie die Master Encryption Keys (MEKs) verwalten und den FIPS 140-2-Modus für die OpenSSL-Verschlüsselung aktivieren bzw. deaktivieren.

WBM-Pfad

WBM **>** *Konfiguration* **>** *Sicherheit*

Das Menü *Sicherheit* wird geöffnet.

Menü *Sicherheit*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

MEK Verwaltung
Sicherheitseinstellungen

3.3.1 MEK Verwaltung

WBM-Pfad

WBM **>** *Konfiguration* **>** *Sicherheit* **>** *MEK Verwaltung*

Der Dialog *Master Encryption Key (MEK) Verwaltung* wird angezeigt. In diesem Dialog können MEKs zu vHG 3575 hinzugefügt oder entfernt werden. Ein MEK ist ein spezieller symmetrischer Schlüssel, der zum Aufbau einer verschlüsselten IP-Verbindung zwischen OpenScape 4000 SoftGate und dem OpenScape 4000 Host System benötigt wird. Er besteht aus genau 16 alphanumerischen Zeichen.

Eingabefeld

In diesem Dialog gibt es das folgende Eingabefeld:

- *MEK [16 Zeichen]:* Hier muss derselbe MEK eingegeben werden, der zuvor im OpenScape 4000 Assistant eingegeben wurde. Es können mehrere MEKs eingegeben werden.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *MEK hinzufügen:* Die in das Eingabefeld *MEK* eingegebenen MEKs werden zu OpenScape 4000 SoftGate hinzugefügt.
- *Alle MEKs entfernen:* Alle zuvor hinzugefügten MEKs werden entfernt.
- *Rückgängig:* Die Eingaben in diesem Fenster werden zurückgesetzt.

Vorgehen

Führen Sie zum Hinzufügen eines MEKs die folgenden Schritte durch:

1. Geben Sie in das Eingabefeld *MEK* die 16 alphanumerischen Zeichen des MEKs ein, den Sie hinzufügen möchten.
2. Klicken Sie auf die Schaltfläche *MEK hinzufügen*. Der MEK wird zur lokalen MEK-Verwaltung hinzugefügt. Wenn einer der MEKs mit dem MEK im OpenScape 4000-System übereinstimmt, kann die Verbindung zwischen vHG 3575 und dem OpenScape 4000-System aufgebaut werden.

3.3.2 Sicherheitseinstellungen

WBM-Pfad

WBM **>** *Konfiguration* **>** *Sicherheit* **>** *Sicherheitseinstellungen*

Der Dialog *Sicherheitseinstellungen* wird angezeigt.

Kontrollkästchen

Dieser Dialog enthält das folgende Kontrollkästchen:

- *FIPS 140-2 aktivieren:* Mit diesem Kontrollkästchen aktivieren bzw. deaktivieren Sie die FIPS 140-2-zertifizierte OpenSSL-Verschlüsselungstechnologie.

  Kontrollkästchen ist aktiviert: Die Payload-Pakete (SRTP) und die SIP-Signalisierungspakete werden mit Hilfe der OpenSSL-Algorithmen nach FIPS-140-2-Standard verschlüsselt.

  FIPS 140-2 ist der gültige Sicherheitsstandard, der die Sicherheitsrichtlinien für Kryptographiemodule festlegt. OpenSSL, die in OpenScape 4000-Produkten verwendete Verschlüsselungstechnologie nutzt Verschlüsselungsalgorithmen und Zertifikate, die nach FIPS 140-2 zertifiziert sind.

  Voraussetzung für die Nutzung der FIPS 140-2-Verschlüsselung ist, dass SPE im SoftGate aktiviert ist. Wenn SPE eingeschaltet und FIPS 140-2 aktiviert ist, dann werden die Payload-Pakete (SRTP) und die SIP-Signalisierungspakete mit Hilfe der OpenSSL-Algorithmen verschlüsselt.

- *Sichere TLS Renegotiation erzwingen (RFC 5746)*: Gilt nur für HFA. Bei TLS ist es möglich, dass ein bösartiger Server über TLS eine Verbindung zu einem Zielserver herstellt, seine Schaddaten überträgt und sich dann in die neue TLS-Verbindung eines Clients einhängt. Bei diesem Vorgang interpretiert der Zielserver den erstmaligen Handshake des Clients als Neuverhandlung einer bestehenden Verbindung, die der bösartige Server zuvor aufgebaut hat. Dabei geht der Zielserver davon aus, dass die in der ersten

Verbindung übertragenen Daten des bösartigen Servers vom Client stammen, der ja nachfolgend seine Daten überträgt. Durch eine sichere Neuverhandlung nach RFC 5746 wird dieses Problem vermieden.

HINWEIS: Änderungen werden erst nach einem Neustart des SoftGates aktiv.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen sind OpenScape Access 500i/a bzw. OpenScape 4000 SoftGate neu zu starten.
- *Rückgängig:* Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt.

3.4 Ansagen/MoH

Im Menü *Ansagen/MoH* können Sie die externen und internen Ansagen und die Einstellungen für die Musik im Wartezustand (Music on Hold, MoH) verwalten.

WBM-Pfad

WBM **>** *Konfiguration* **>** *Ansagen/MoH*

Das Menü *Ansagen/MoH* wird geöffnet.

Menü *Ansagen/MoH*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

Externe Ansagen
Interne Ansagen

3.4.1 Externe Ansagen

WBM-Pfad

WBM **>** *Konfiguration* **>** *Ansagen/MoH*

Der Dialog *Externe Ansagen verwalten* wird angezeigt.

In diesem Dialog können die Einstellungen für die Ansagebaugruppe, auf der die Ansagen gespeichert sind, vorgenommen werden.

Eingabefelder

In diesem Dialog gibt es die folgenden Eingabefelder:

- *Slot-Circuit:* Nur Slots mit konfigurierten vSLAM und vTMOM werden in der Klappliste angezeigt.
- *Dateiname:* In dieses Eingabefeld sind der Pfad und der Name der Datei einzugeben, welche die Ansage enthält (wav-Datei im Format „PCM16, 8 kHz, mono“). Über die Schaltfläche *Durchsuchen* kann die Datei auch ausgewählt werden.

HINWEIS: Während des Ladevorgangs wird die wav-Datei dahingehend überprüft, ob sie ein gültiges Format hat und ob alle Einschränkungen (PCM16, 8 kHz, mono) erfüllt werden.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Laden:* Die angegebene Datei wird geladen.
- *Rückgängig:* Der eingegebene Pfad und der Dateiname werden gelöscht.

- *Löschen:* Die betreffende Ansage in der Tabelle *Dateiname*/*Aktion* wird gelöscht.

Tabelle *Dateiname*/*Aktion*

In dieser Tabelle werden die geladenen Ansagen angezeigt.

Vorgehen

Führen Sie zum Laden einer Ansage die folgenden Schritte durch:

1. Geben Sie in das Eingabefeld *Circuit (0-255)* den erforderlichen Wert ein.
2. Geben Sie den Pfad und den Namen der Datei ein, welche die Ansage enthält oder wählen Sie über die Schaltfläche *Durchsuchen* die Datei aus.
3. Klicken Sie auf die Schaltfläche *Laden*. Die Datei wird geladen und in der Tabelle *Dateiname/Aktion* angezeigt.

3.4.2 Interne Ansagen

WBM **>** *Konfiguration* **>** *Ansagen/MoH* > *Interne Ansagen*

Der Dialog *Interne MoH Einstellung* wird angezeigt.

Schaltflächen und Kontrollkästchen

In diesem Dialog gibt es die folgenden Kontrollkästchen und Schaltflächen:

- *Klassische interne MoH aktivieren*: Mit diesem Kontrollkästchen aktivieren bzw. deaktivieren Sie das Leistungsmerkmal *Klassische interne Musik im Wartezustand (MoH)*.
- *Übernehmen:* Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen sind OpenScape Access 500i/a bzw. OpenScape 4000 SoftGate neu zu starten.
- *Rückgängig:* Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt.

3.5 WAN

Im Menü *WAN* können Sie die Einstellungen für die WAN-Schnittstelle und für die SPE-Zertifikate konfigurieren.

WBM-Pfad

WBM **>** *Konfiguration* **>** *WAN*

Das Menü *WAN* wird geöffnet.

Menü *WAN*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

Einstellungen
SPE

3.5.1 Einstellungen

WBM-Pfad

WBM **>** *Konfiguration* **>** *WAN* **>** *Einstellungen*

Der Dialog *WAN Einstellungen* wird angezeigt.

In diesem Dialog können Sie die Einstellungen für die WAN-Schnittstelle konfigurieren und den Zugriff auf die Telefonbilder über WAN aktivieren bzw. deaktivieren.

Auswahl- und Eingabefelder, Kontrollkästchen

In diesem Dialog gibt es die folgenden Eingabefelder:

- *Redundantes WAN - ein/aus:* Redundanz für das Management LAN aktivieren/deaktivieren. Wählen Sie aus der Dropdown-Liste die gewünschte Einstellung. Standardeinstellung: aus (deaktiviert).
- *WAN Interface - Deaktiviert* oder *eth0*, *eth3* bis *eth7:* WAN-Interface deaktivieren oder gewünschte Ethernet-Schnittstelle auswählen. Wählen Sie aus der Dropdown-Liste die gewünschte Einstellung. Standardeinstellung: Deaktiviert.

Kontrollkästchen

Dieser Dialog enthält das folgende Kontrollkästchen:

- *Telefonbilderzugriff für WAN aktivieren (Picture CLIP):*
  Durch Aktivieren/Deaktivieren dieses Kontrollkästchens legen Sie fest, ob der Zugriff über das WAN auf Telefonbilder, die auf externen Servern gespeichert sind, freigegeben bzw. blockiert werden soll.

Um die Parameter für dieses Leistungsmerkmal zu konfigurieren, wählen Sie die Menüoption *Picture CLIP* in der Navigationsleiste. Details hierzu finden Sie unter *Picture CLIP*.

HINWEIS: Änderungen werden erst nach einem Neustart des SoftGates aktiv.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen sind OpenScape Access 500i/a bzw. OpenScape 4000 SoftGate neu zu starten.
- *Rückgängig:* Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt.

3.5.2 SPE

Durch SPE (Signaling & Payload Encryption) werden VoIP-Nutz- und Signalisierungsdatenströme von und zur vHG 3575/vHG 3500 HFA verschlüsselt. Diesem Leistungsmerkmal liegt ein asymmetrisches Verschlüsselungsverfahren zugrunde. Bei einem solchen Verfahren werden öffentliche und private Schlüssel verwendet.

Es muss gewährleistet werden, dass sich die einzelnen VoIP-Clients sowie die Gateways, z. B. vHG 3575, im Kommunikationssystem eindeutig identifizieren. Dies wird durch Zertifikate erreicht, die private oder öffentliche Schlüssel enthalten. Die Zertifikate werden entweder durch eine Kunden PKI-Zertifizierungsstelle (RA/CA) oder durch die interne Zertifizierungsstelle des DLS-Servers (CA) erzeugt. Der DLS-Server sendet dann die Dateien, die diese Zertifikate enthalten, an den DLS-Client des Gateways.

Je nach Bedarf können Sicherheitseinstellungen für die Auswertung der Zertifikate und für die Verschlüsselung der Datenströme aktiviert oder deaktiviert werden. Dadurch wird die Sicherheit der Verschlüsselung erhöht oder verringert.

WBM-Pfad

WBM **>** *Konfiguration* **>** *WAN* **>** *SPE*

Das Menü *SPE* wird geöffnet.

Menü *SPE*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

Keycert importieren
Keycert anzeigen
Keycert löschen
SPE Sicherheitseinstellungen

3.5.2.1 Keycert importieren

HINWEIS: Wenn Sie bei aktiviertem SPE das erste Mal ein Zertifikat importieren, wird anschließend automatisch ein Reset durchgeführt.

WBM-Pfad

WBM **>** *Konfiguration* **>** *WAN* **>** *SPE* **>** *Keycert importieren*

Der Dialog *Laden eines SPE Key Zertifikats über HTTP* wird angezeigt. In diesem Dialog kann ein SPE Key Zertifikat durch Eingeben des Entschlüsselungskennworts und des Dateinamens importiert werden. Die Datei, welche das Zertifikat enthält, stammt von einer Kunden PKI-Zertifizierungsstelle (RA/CA) oder der internen Zertifizierungsstelle (CA) des DLS-Servers und muss im PEM- oder im PKCS#12-Format vorliegen.

Eingabefelder

In diesem Dialog gibt es die folgenden Eingabefelder:

- *Entschlüsselungskennwort*: In dieses Feld ist das Kennwort einzugeben, das bei der Erstellung der PEM- oder PKCS#12-Datei verwendet wurde.
- *Datei mit Zertifikat und privatem Schlüssel (PEM- oder PKCS#12-Format)*: In dieses Eingabefeld sind der Pfad und der Name der Datei, die das Zertifikat enthält, einzugeben. Über die Schaltfläche *Durchsuchen* kann die Datei auch ausgewählt werden.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Fingerabdruck des Zertifikats anzeigen*: Durch Prüfen des Fingerabdrucks kann festgestellt werden, ob ein unverändertes Zertifikat vorliegt oder ob es verändert wurde.
- *Zertifikat aus Datei importieren*: Das Zertifikat wird aus der im oben genannten Eingabefeld angegebenen Datei importiert.

Vorgehen

Führen Sie zum Laden eines SPE-Zertifikats die folgenden Schritte durch:

1. Wählen Sie: *WBM* **>** *Konfiguration* **>** *WAN* **>** *SPE* **>** *Keycert importieren.* Der Dialog *Laden eines SPE Key Zertifikats über HTTP* wird angezeigt. Folgende Felder können Sie bearbeiten:
    - *Entschlüsselungskennwort*: Geben Sie in diesem Feld das Kennwort ein, das bei der Erstellung der PEM- oder PKCS#12-Datei verwendet wurde.

- *Datei mit Zertifikat und privatem Schlüssel (PEM oder PKCS#12-Format)*: Geben Sie den Pfad und den Dateinamen der Datei ein, die die zu importierenden Zertifikats-Daten enthält. Klicken Sie auf *Durchsuchen*, um einen Dialog zur Suche nach der Datei zu öffnen.

2. Klicken Sie auf *Fingerabdruck des Zertifikats anzeigen*. Ein Fenster mit dem Fingerabdruck des zu importierenden Zertifikats wird angezeigt:

   a) Prüfen Sie den Fingerabdruck (hexadezimale Zahl). Wenn ein Zertifikat verändert wurde, ändert sich immer der Fingerabdruck. Nur ein unveränderter Fingerabdruck ist eine Gewähr für ein unverändertes Zertifikat. Sind die beiden Fingerabdrücke nicht identisch, dann liegt wahrscheinlich ein Angriffsversuch vor. In diesem Fall darf der Schlüssel nicht mehr verwendet werden; darüber hinaus sind die festgelegten Maßnahmen zu ergreifen.

   b) Klicken Sie auf *OK*, um das Fenster mit dem Fingerabdruck zu schließen.

3. Klicken Sie auf *Zertifikat aus Datei importieren*, wenn Sie mit der Prüfung des Fingerabdruck zufrieden sind. Importieren Sie das Zertifikat nicht, falls der Fingerabdruck nicht Ihren Erwartungen entspricht.

3.5.2.2 Keycert anzeigen

WBM-Pfad

WBM **>** *Konfiguration* **>** *WAN* **>** *SPE* **>** *Keycert anzeigen*

Der Dialog *Zertifikatsinformationen* wird angezeigt. In diesem Dialog kann das SPE-Zertifikat angezeigt werden, z. B. um es zu überprüfen.

Angezeigte Daten

Es werden die folgenden Daten aus dem Zertifikat angezeigt:

- Allgemeine Daten: *Name des Zertifikats*, *Zertifikatstyp*, *Seriennummer des Zertifikats*, *Seriennummer des Zertifikats (hex)*, *Signatur-Algorithmus-Typ*, *Beginn der Zertifikatsgültigkeit (GMT)*, *Ende der Zertifikatsgültigkeit (GMT)*, *CRL-Verteilungspunkt*
- *Ausgestellt durch CA*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name (CN)*
- *Antragsteller*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name (CN)*
- *Alternativer Antragstellername*
- *Daten des öffentl. Schlüssels*: *Länge des öffentl. Schlüssels*, *Öffentlicher Schlüssel*, *Fingerabdruck*

3.5.2.3 Keycert löschen

WBM-Pfad

WBM **>** *Konfiguration* **>** *WAN* **>** *SPE* **>** *Keycert löschen*

Der Dialog *Zertifikat für SPE löschen* wird angezeigt. In diesem Dialog kann das SPE-Zertifikat gelöscht werden, z.B. wenn ein neues Zertifikat benötigt wird.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Löschen*: Das SPE-Zertifikat kann nach einer Warnung gelöscht werden.
- *Abbrechen*: Der Löschvorgang wird abgebrochen.

Vorgehen

Führen Sie zum Löschen des SPE-Zertifikats die folgenden Schritte durch:

1. Wählen Sie: *WBM* **>** *Konfiguration* **>** *WAN* **>***SPE* **>** *Keycert löschen*. Eine Warnung wird angezeigt. Zur Kontrolle wird außerdem der Name des Zertifikats angegeben.
2. Klicken Sie auf *Löschen* und im Bestätigungsdialog auf *OK*.

3.5.2.4 SPE Sicherheitseinstellungen

WBM-Pfad

WBM **>** *Konfiguration* **>** *WAN* **>***SPE* **>** *SPE Sicherheitseinstellungen*

Der Dialog *SPE Sicherheitseinstellungen* wird angezeigt. In diesem Dialog können die Sicherheitseinstellungen für Signaling- und Payload Encryption (SPE) an die Sicherheitsbedürfnisse des Kunden angepasst werden. Dies betrifft die Verschlüsselung der Signalisierungs- und der Nutzdaten bei der Kommunikation zwischen der vHG 3575/vHG 3500 HFA und den VoIP-Clients sowie zwischen zwei vHG 3575.

Auswahl- und Eingabefelder, Kontrollkästchen

In diesem Dialog gibt es die folgenden Einstellungen:

- *Maximales Intervall für Schlüssel-Neuverhandlung [Stunden]*: Dieser Wert gibt an, wie lange ein bestimmter Schlüssel für die Verschlüsselung der Signalisierungs- und Nutzdaten verwendet werden soll. Nach Ablauf dieser Zeitdauer wird ein neuer Schlüssel festgelegt.
- *Salt Key Verfahren verwenden*: Mit diesem Verfahren können Passworter stark verschlüsselt werden. Deren Entschlüsselung kann dadurch wesentlich erschwert oder sogar weitestgehend unmöglich gemacht werden. So ist zum Beispiel nach einer Verschlüsselung nicht mehr erkennbar, ob zwei Benutzer das gleiche Passwort verwenden.

- *SRTP Authentifizierung notwendig* (SRTP: Secure Real-time Transport Protocol): Durch die SRTP-Authentifizierung werden Nutzdatenfälschungen und Replay-Attacken vermieden. Dazu wird überprüft:
  - ob die Nutzdaten-Message eines VoIP-Clients unverfälscht ist.
  - ob eine Nutzdaten-Message bereits einmal empfangen wurde.
- *SRTCP Verschlüsselung notwendig* (SRTCP: Secure Real-time Transport Control Protocol): Durch die SRTCP-Verschlüsselung werden Fälschungen der Signalisierungsdaten und Replay-Attacken vermieden. Überprüft wird:
  - ob die Signalisierungsdaten-Message des VoIP-Clients unverfälscht ist.
  - ob eine Signalisierungsdaten-Message bereits einmal empfangen wurde.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert.
- *Rückgängig:* Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt.

Vorgehen

Um die SPE-Sicherheitseinstellungen zu ändern, gehen Sie wie folgt vor:

1. Wählen Sie: *WBM* **>** *Konfiguration* **>** *WAN* **>***SPE* **>** *SPE Sicherheitseinstellungen*. Der Dialog *SPE Sicherheitseinstellung ändern* wird angezeigt.
2. Nehmen Sie die gewünschten Einstellungen vor, siehe Absatz *Auswahl- und Eingabefelder, Kontrollkästchen*.
3. Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*. Die geänderten Daten werden in die Konfiguration übernommen.

3.6 LAN Interfaces

Mittels der Einstellungen in diesem Menü kann das Voice-LAN vollständig von den Management-, XLink-, HFA- und SIP-Interfaces getrennt werden. Zudem kann ein alternativer LAN-Weg für die Übertragung der Signalisierungsdaten eingestellt werden.

WBM-Pfad

WBM **>** *Konfiguration* **>** *LAN Interfaces*

Das Menü *LAN Interfaces* wird geöffnet:

Menü *LAN Interfaces*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

Management Interface
Signalling Survivability Interface
XLink
HFA Interface
SIP Interface

3.6.1 Management Interface

RQ00033881

Mit der Einführung des Leistungsmerkmals "Separate LAN-Konnektivität für Administration und VoIP" kann das Voice-LAN vollständig vom Management-LAN getrennt werden. Zuvor war es lediglich möglich, das IPDA-LAN vom Kunden-LAN zu trennen.

Wenn Sie das Management-LAN vom Voice-LAN trennen möchten, müssen Sie eine IP-Adresse für das Management-LAN angeben. Im WBM wird nur das LAN-Interface angegeben, auf dem die IP-Adresse für das Management-LAN eingerichtet ist bzw. eingerichtet werden soll, die IP-Adresse selbst wird im RMX-Teil mittels AMO STMIB angegeben.

Wenn eine IP-Adresse für das Management-LAN angegeben ist, verwendet OpenScape 4000 Assistant diese für die Verbindung zum Gateway-WBM über die Kunden-LAN-Schnittstelle. Wenn die IP-Adresse auf den Standardwert 0.0.0.0 eingestellt ist, verwendet OpenScape 4000 Assistant die IP-Adresse das IPDA-LAN.

Die Trennung der beiden Interfaces kann über das Gateway konfiguriert werden.

Die Menüoption *Management Interface* ermöglicht es Ihnen, die Management LAN-Schnittstelle zu aktivieren bzw. zu deaktivieren und die Einstellungen für das Management-LAN zu konfigurieren.

WBM-Pfad

WBM **>** *Konfiguration* **>** *LAN Interfaces* **>** *Management Interface*

Der Dialog *Management Interface Einstellungen* wird angezeigt. In diesem Dialog können Sie das Management LAN Interface aktivieren bzw. deaktivieren und die Redundanz für das Management LAN ein- bzw. ausschalten.

Auswahlfelder

In diesem Dialog gibt es die folgenden Auswahlfelder:

- *Redundantes Management LAN*: Das redundante Management LAN-Interface kann ein- oder ausgeschaltet werden. Wählen Sie im Auswahlfeld die gewünschte Einstellung aus:
  - Mögliche Werte: *ein*, *aus*
  - Voreinstellung: *aus* (deaktiviert)
- *Management LAN Interface*: Das Management LAN-Interface kann deaktiviert oder die dafür verwendete LAN/Ethernet-Schnittstelle ausgewählt werden.Wählen Sie im Auswahlfeld die gewünschte Einstellung aus:
  - Mögliche Werte: *Deaktiviert*, *eth0*, *eth2*, *eth3*, *eth4*, *eth5*, *eth6*, *eth7*
  - Voreinstellung: *Deaktiviert*

WICHTIG: Für das IPDA-Interface und das Management-Interface darf nicht dieselbe LAN/Ethernet-Schnittstelle verwendet werden!

WICHTIG: Damit alle Konfigurationsänderungen wirksam werden, muss OpenScape 4000 SoftGate bzw. OpenScape Access 500i/a bzw. neu gestartet werden.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen sind OpenScape Access 500i/a bzw. OpenScape 4000 SoftGate neu zu starten.
- *Rückgängig:* Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt.

3.6.2 Signalling Survivability Interface

RQ00031771

"Signaling Survivability über alternatives LAN" schaltet im Störungsfall die Steuerungsverbindung vom IP-Netz auf einen alternativen LAN-Weg um. Die Umschaltung des Signalisierungspfades erfolgt unterbrechungsfrei.

Zusätzlich zu der Konfiguration mit den AMOs muss für die vHG 3575 im OpenScape 4000 SoftGate die LAN-Schnittstelle ausgewählt werden, die für Signaling Survivability genutzt werden soll.

Die Menüoption *Signalling Survivability Interface* ermöglicht es Ihnen, die Einstellungen für das Signalling Survivability Interface zu konfigurieren.

WBM-Pfad

WBM **>** *Konfiguration* **>** *LAN Interfaces* **>** *Signalling Survivability Interface*

Der Dialog *Signalling Survivability Interface Einstellungen* wird angezeigt. In diesem Dialog können Sie das LAN Interface angeben und die LAN-Redundanz ein- bzw. ausschalten. Darüber hinaus werden in diesem Dialog die internen IP-Adressen der TUN-Devices für die HSR-Verbindung angezeigt (HSR: High-availability Seamless Redundancy).

Auswahlfelder

In diesem Dialog gibt es die folgenden Auswahlfelder:

- *Redundantes LAN*: Die LAN-Redundanz für die Schnittstelle kann aktiviert bzw. deaktiviert werden. Wählen Sie im Auswahlfeld die gewünschte Einstellung aus:
  - Mögliche Werte: *ein*, *aus*
  - Voreinstellung: *aus* (deaktiviert)
- *LAN Interface*: Das Signalling Survivability LAN-Interface kann deaktiviert oder die dafür verwendete LAN/Ethernet-Schnittstelle ausgewählt werden.Wählen Sie im Auswahlfeld die gewünschte Einstellung aus:
  - Mögliche Werte: *Deaktiviert*, *eth0*, *eth2*, *eth3*, *eth4*, *eth5*, *eth6*, *eth7*
  - Voreinstellung: *eth2*

Eingabefelder unter *Interne IP Adressen der TUN-devices für die HSR Verbindung (Experten-Einstellungen)*

Für das spezifische Routing über eine HSR-Verbindung via interne TUN-Geräte sind zwei host-interne IP-Adressen erforderlich.

Die Standardeinstellungen sollten nicht geändert werden, solange es keine anderen äquivalenten externen IP-Adressen gibt, die für den Host erreichbar sein müssen.

Da die Standardeinstellungen einem reservierten Bereich angehören, sollte dieser Fall nicht allzu häufig auftreten.

In diesem Dialog gibt es die folgenden Anzeigefelder:

- *IP-Adresse für TUN-Device #1*: Interne IP-Adresse des TUN-Device #1 für die HSR-Verbindung.

- *IP-Adresse für TUN-Device #2*: Interne IP-Adresse des TUN-Device #2 für die HSR-Verbindung.

WICHTIG: Damit alle Konfigurationsänderungen wirksam werden, muss OpenScape 4000 SoftGate bzw. OpenScape Access 500i/a bzw. neu gestartet werden.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen sind OpenScape Access 500i/a bzw. OpenScape 4000 SoftGate neu zu starten.
- *Rückgängig:* Die Eingaben werden verworfen und auf die Voreinstellung zurückgesetzt.

3.6.3 XLink

XLink (X-LINK) dient zur Anbindung der OpenScape Access Module SLA, SLO, BRI, PRI, SLC und TA an OpenScape Access 500i/a bzw. an OpenScape 4000 SoftGate. Diese sind wiederum über die I und C Infrastruktur (1 Gigabit-LAN) mit OpenScape 4000 V8 verbunden. In OpenScape Access 500i/a und OpenScape 4000 SoftGate ist jeweils eine Applikation OpenScape 4000 SoftGate integriert.

Durch XLink und das 1 Gigabit-LAN wird die erforderliche hohe Bandbreite für die Übertragung des Sprachverkehrs, d.h. der Nutzdaten, zur Verfügung gestellt.

WBM-Pfad

WBM **>** *Konfiguration* **>** *LAN Interfaces* **>** *XLink*

Der Dialog *XLINK Einstellungen* wird angezeigt. In diesem Dialog können Sie das XLink LAN-Interface deaktivieren oder die dafür verwendete LAN/Ethernet-Schnittstelle auswählen sowie die XLink-Netzwerk-Adresse eingeben.

Auswahl- und Eingabefelder

In diesem Dialog gibt es die folgenden Auswahl-/Eingabefelder:

- *XLink LAN Interface*: Das XLink LAN-Interface kann deaktiviert oder die dafür verwendete LAN/Ethernet-Schnittstelle ausgewählt werden.Wählen Sie im Auswahlfeld die gewünschte Einstellung aus:
  - Mögliche Werte: *Deaktiviert*, *eth0*, *eth1*, *eth3*, *eth4*, *eth5*, *eth6*, *eth7*
  - Voreinstellung: *eth1*

- *XLink Netzwerk-Adresse*: Es muss die IP-Adresse eines Netzwerks eingegeben werden, d.h. die letzten beiden Stellen müssen „.0.0“ sein, z.B. „10.100.0.0“.

WICHTIG: Damit alle Konfigurationsänderungen wirksam werden, muss OpenScape 4000 SoftGate bzw. OpenScape Access 500i/a bzw. neu gestartet werden.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen sind OpenScape Access 500i/a bzw. OpenScape 4000 SoftGate neu zu starten.
- *Rückgängig:* Die Eingaben werden verworfen und auf die Voreinstellung zurückgesetzt.

3.6.4 HFA Interface

Das HFA-Interface dient der Bereitstellung von OpenScape 4000 Leistungsmerkmalen in einer IPDA (HFA: HiPath Feature Access, IPDA: Internet Protocol Distributed Architecture).

WBM-Pfad

WBM **>** *Konfiguration* **>** *LAN Interfaces* **>** *HFA Interface*

Der Dialog *HFA Interface Einstellungen* wird angezeigt. In diesem Dialog können Sie das HFA-Interface ein- oder ausschalten und die dafür verwendete LAN/Ethernet-Schnittstelle auswählen.

Auswahl- und Eingabefelder

In diesem Dialog gibt es die folgenden Auswahlfelder:

- *Redundantes HFA LAN*: Das redundante HFA-Interface kann ein- oder ausgeschaltet werden. Wählen Sie im Auswahlfeld die gewünschte Einstellung aus:
  - Mögliche Werte: *ein*, *aus*
  - Voreinstellung: *aus* (deaktiviert)
- *HFA LAN Interface*: Die gewünschte Ethernet-Schnittstelle kann ausgewählt werden. Wählen Sie im Auswahlfeld die gewünschte Ethernet-Schnittstelle aus:
  - Mögliche Werte: *Default IPDA*, *eth0*, *eth3*, *eth4*, *eth5*, *eth6*, *eth7*

– Voreinstellung: *Default IPDA*

WICHTIG: Für das HFA-Interface und das Management-Interface darf nicht dieselbe LAN/Ethernet-Schnittstelle verwendet werden!

WICHTIG: Damit alle Konfigurationsänderungen wirksam werden, muss OpenScape 4000 SoftGate bzw. OpenScape Access 500i/a bzw. neu gestartet werden.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen sind OpenScape Access 500i/a bzw. OpenScape 4000 SoftGate neu zu starten.
- *Rückgängig:* Die Eingaben werden verworfen und auf die Voreinstellung zurückgesetzt.

3.6.5 SIP Interface

Das SIP-Interface dient dem Aufbau, der Steuerung und dem Abbau von Kommunikationssitzungen mit Hilfe des SIP in einer IPDA (SIP: Session Initiation Protocol, IPDA: Internet Protocol Distributed Architecture).

WBM-Pfad

WBM **>** *Konfiguration* **>** *LAN Interfaces* **>** *SIP Interface*

Der Dialog *SIP Interface Einstellungen* wird angezeigt. In diesem Dialog können Sie das SIP-Interface ein- oder ausschalten und die dafür verwendete LAN/Ethernet-Schnittstelle auswählen.

Auswahl- und Eingabefelder

In diesem Dialog gibt es die folgenden Auswahlfelder:

- *Redundantes SIP LAN*: Das redundante SIP-Interface kann ein- oder ausgeschaltet werden. Wählen Sie im Auswahlfeld die gewünschte Einstellung aus:
  - Mögliche Werte: *ein*, *aus*
  - Voreinstellung: *aus* (deaktiviert)
- *SIP LAN Interface*: Die gewünschte Ethernet-Schnittstelle kann ausgewählt werden. Wählen Sie im Auswahlfeld die gewünschte Ethernet-Schnittstelle aus:

– Mögliche Werte: *Default IPDA*, *eth0*, *eth3*, *eth4*, *eth5*, *eth6*, *eth7*

– Voreinstellung: *Default IPDA*

WICHTIG: Für das SIP-Interface und das Management-Interface darf nicht dieselbe LAN/Ethernet-Schnittstelle verwendet werden!

WICHTIG: Damit alle Konfigurationsänderungen wirksam werden, muss OpenScape 4000 SoftGate bzw. OpenScape Access 500i/a bzw. neu gestartet werden.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen sind OpenScape Access 500i/a bzw. OpenScape 4000 SoftGate neu zu starten.
- *Rückgängig:* Die Eingaben werden verworfen und auf die Voreinstellung zurückgesetzt.

3.7 Diverse

WBM-Pfad

WBM **>** *Konfiguration* **>** *Diverse*

Das Menü *Diverse* wird geöffnet:

Menü *Diverse*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

Fax-Parameter
NGS
QoS-Data-Collection

3.7.1 Fax-Parameter

WBM-Pfad

WBM **>** *Konfiguration* **>** *Diverse* **>** *Fax-Parameter*

Der Dialog *Fax-Parameter* wird angezeigt. In diesem Dialog können die Fax-Parameter für T.38-Fax festgelegt werden. Aufgrund der ITU-T Empfehlung T.38 ist es möglich, über ein paketvermitteltes Netz, z. B. das Internet, Faxe in Echtzeit zu übertragen. Dazu wird das IFP (Internet Facsimile Protocol), welches auf UDP bzw. TCP und IP aufsetzt, verwendet (UDP: User Datagram Protocol, TCP: Transmission Control Protocol).

Auswahl- und Eingabefelder, Kontrollkästchen

In diesem Dialog gibt es die folgenden Einstellungen:

- T.38 Fax:
  - *Max. UDP-Datagramm-Größe (Byte):* Maximale Größe eines T.38-UDP-Datagramms in Bytes.
  - *Verwendete Fehlerkorrektur (UDP):* Legt fest, welche Methode zur Fehlerkorrektur eingesetzt werden soll (*t38UDPRedundancy* oder *t38UDPFEC*).
  - *Fehler-Korrektur-Modus*: Wenn dieses Kontrollkästchen aktiviert ist, wird einer von 2 möglichen Fehlerkorrekturmechanismen ausgewählt, die das T.38 Fax-Protokoll über UDP zur Verfügung stellt. Beide Mechanismen dienen dazu, dass eine Faxübertragung auch bei begrenzten Paketverlusten im Netzwerk fehlerfrei abläuft.
  - *Fax-Kanal mit ermitteltem Ton öffnen:* Wählton, welcher vom vHG 3575 an das Faxgerät gesendet wird. Danach wählt das Faxgerät die Rufnummer.

  - *Anzahl redundanter Pakete:* Es kann ausgewählt werden, wie viele redundante Pakete bei den Fehlerkorrekturmechanismen ausgewählt werden. Je größer dieser Wert ist, desto robuster ist die Faxübertragung gegenüber Paketverlusten auf dem Netzwerk. Dafür steigt bei größeren Werten die benötigte Bandbreite an. Auswählbare Werte: 0, 1, 2
  - *Maximaler Netzwerk-Jitter (ms)*: Wenn der maximale Jitter im Netzwerk bekannt ist, dann geben Sie ihn in diesem Feld ein. Dadurch verkürzt sich die Übertragungszeit bei einigen Faxgeräten. Der Wert muss als Dezimalzahl eingegeben werden. Wertebereich: 140 ms - 500 ms. Default: 200 ms.

- Sonstiges:
  - *ClearMode (ClearChannelData)*: Es kann festgelegt werden, ob der Clear Channel Codec nach RFC 4040 in den RTP-Datenpaketen zu verwenden ist.
  - *Rahmengröße*: Die Größe des Rahmens für den Clear Channel Codec kann festgelegt werden.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert.
- *Rückgängig:* Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt.

Vorgehen

Führen Sie zum Festlegen der Fax-Parameter die folgenden Schritte durch:

1. Nehmen Sie die gewünschten Einstellungen vor, siehe Absatz „*Auswahl- und Eingabefelder, Kontrollkästchen*“.
2. Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK*. Die geänderten Daten werden in die Konfiguration übernommen.

3.7.2 NGS

Die Webservice-Lösung NextGen-Service (NGS) überträgt die IPv4- und/oder IPv6-Adressen sowie alle übrigen für die Routing-Informationen benötigten Daten vom SoftGate zum NGS-Server.

WBM-Pfad

WBM **>** *Konfiguration* **>** *Diverse* **>** *NGS*

Der Dialog *NGS Einstellungen* wird angezeigt. In diesem Dialog geben Sie die IP-Adresse des NGS-Servers ein.

WICHTIG: Damit alle Konfigurationsänderungen wirksam werden, muss OpenScape 4000 SoftGate bzw. OpenScape Access 500i/a bzw. neu gestartet werden.

Eingabefelder

In diesem Dialog gibt es die folgenden Eingabefelder:

- *IP-Adresse des NGS-Servers [IPv4 oder IPv6]*: Die IP-Adresse kann im Format IPv4 oder IPv6 eingegeben werden. Standardformat ist IPv4: 0.0.0.0.
- Use NGS Client (NGS-Client verwenden): Standard True: Sie haben die Möglichkeit, den internen SoftGate NGS-Client zu deaktivieren, wenn das SoftGate den zentralen NGS-Server nicht erreichen kann (z. B.beim Betrieb in einem DMZ).

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen sind OpenScape Access 500i/a bzw. OpenScape 4000 SoftGate neu zu starten.
- *Rückgängig:* Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt.

3.7.3 QoS-Data-Collection

RQ00033039

Quality of Service Data Collection (QDC) – Aufgaben und Funktionen:

Mit dem OpenScape IP-Service „QoS-Data-Collection” steht ein Tool zur Verfügung, das Daten von OpenScape-Produkten sammelt, um diese auf Sprach- und Netzwerk-Qualität zu analysieren.

Ziele des „QoS-Data-Collection” Service mit seinen Leistungsmerkmalen sind:

- Reduzierung der allgemeinen Aufwendungen bei der Analyse von QoS-Problemen.
- Erhöhung der „remote clearance rate”.
- Frühzeitiges Erkennen von Netzwerkproblemen zur Vorbeugung gegen Störungen der Sprachqualität.

Das führt zu:

- Reduzierung der Service-Aufwendungen und Kosten.
- Konkurrenzfähigen Wartungsverträgen.
- Schnellen und qualifizierten Antworten zu einem Kundenproblem.
- Erhöhung der allgemeinen Kundenzufriedenheit mit dem Produkt und der Technologie.
- Der Möglichkeit, Änderungen in der Netzwerkumgebung des Kunden zu erkennen und die Marketing-Aktivitäten von OpenScape-Services entsprechend auszurichten.

Durch den Einsatz von QDC können wichtige Verbesserungen im gesamten Service-Prozess (break/fix process) erzielt werden.

Hintergrundinformationen zu QDC

Siehe *OpenScape 4000 V7 Gateways HG 3500 und HG 3575, Administratordokumentation.*

WBM-Pfad

WBM **>** *Konfiguration* **>** *Diverse* **>** *QoS-Data-Collection*

Der Dialog *Quality of Service Data Collection* wird angezeigt.

Auswahl- und Eingabefelder

Folgende Felder können Sie bearbeiten:

QDC-Konfiguration

- *Senden an QCU*: Aktivieren Sie dieses Kontrollkästchen, wenn Daten an die QCU gesendet werden sollen.
  Standardwert: Kontrollkästchen nicht aktiviert.
- *QCU-IP-Adresse*: Geben Sie hier die IP-Adresse oder den Namen des QCU-Host ein.
  Standardwert: 0.0.0.0.
- *QCU-Empfangsport*: Empfangsport der QCU. Geben Sie hier die Portnummer des QCU-Host ein.
  Standardwert: 12010.
- *Senden an Network Management aktiv*: Aktivieren Sie dieses Kontrollkästchen, wenn Daten an das Network Management gesendet werden sollen.
  Standardwert: Kontrollkästchen nicht aktiviert.
- *IP-Adresse des Network Managements*: Geben Sie hier die IP-Adresse oder den Namen ein.
  Standardwert: 0.0.0.0.

- *Community String*: n/a

WICHTIG: Wenn eines der Kontrollkästchen **Senden an QCU** oder **Senden an Network Management** aktiviert ist (Haken gesetzt) werden QoS-Reports erzeugt.

QDC-Reportmodus

- *Sende Bericht, wenn*: Wählen Sie aus dem Listenfeld den gewünschten Zeitpunkt zur Berichtübertragung aus. Folgende Möglichkeiten stehen Ihnen zur Auswahl:
  - *Session-Ende und Schwellwert überschritten*: Ein Report wird nur am Ende einer Session gesendet und nur wenn der Schwellwert erreicht wurde.
  - *Ende des Berichtsintervalls und Schwellwert überschritten*: Ein Report wird in jedem Berichtsintervall gesendet wenn der Schwellwert erreicht wurde.
  - *Session-Ende, unbedingt*: Am Session-Ende wird immer ein Report gesendet.
  - *Ende des Berichtsintervalls, unbedingt*: Am Ende des Berichtsintervalls wird immer ein Report gesendet.
- *Berichtsintervall (s)*: Geben Sie hier den Berichtsintervall in sec. ein, in dem Berichte gesendet werden. Für jeden Berichtsintervall wird ein QoS-Report gesendet wenn der Reportmodus entsprechend gesetzt wurde.
  Standardwert: 60 sec.
  Gültige Werte: 0 ... 65535
- *Beobachtungszeitraum (s)*: Nicht einstellbarer Parameter.
  Standardwert: 10 sec.
- *Minimale Session-Dauer (* 100 ms)*: Geben Sie hier die minimale Session-Dauer mal 100ms an. Besteht eine Session (z.B. eine Gesprächsverbindung) kürzer als dieses Minimum, dann wird kein QoS Report gesendet.
  Standardwert: 20 (2 sec)
  Gültige Werte: 0 ... 255

WICHTIG: Die Zeitskala ist im Beobachtungszeitraum und im Berichtsintervall segmentiert. Jeder Beobachtungszeitraum wird auf eine Schwellwertüberschreitung geprüft. Für jeden Berichtsintervall wird ein QoS-Report gesendet, wenn der Reportmodus entsprechend gesetzt wurde.

QDC-Schwellwerte

- *Oberer Jitter-Schwellwert (ms)*: Geben Sie hier den oberen Jitter-Schwellwert für die Reportauslösung ein. Der Jitter wird gegen diesen Schwellwert geprüft und zwischen zwei aufeinanderfolgenden RTP Paketen gemessen.
  Standardwert: 20ms
  Gültige Werte: 0 ... 255

- *Schwellwert für durchschn. Paketlaufzeitverzögerung (ms)*: Paketlaufzeitverzögerung ist die Summe der Laufzeiten in beide Richtungen. , ; geben Sie in dieses Feld den Schwellwert für die durchschnittliche Paketlaufzeitverzögerung ein, der die Reportauslösung bewirkt.
  Standardwert: 100ms
  Gültige Werte: 0 ... 65535

- *Schwellwerte für Komprimierungs-Codec*: Geben Sie hier die gewünschte Anzahl in Paketen der Schwellwerte für die Komprimierungs-Codec ein. Folgende Möglichkeiten stehen Ihnen zur Auswahl:

  - *verlorene Pakete (pro 1000 Pakete)*: Geben Sie hier den Schwellwert für die Pakete ein, welche bei der Sprachdecodierung verlorengegangen sind. Der Wert ist das Verhältnis von verlorenen Paketen zur Gesamtzahl der Pakete.
    Standardwert: 10
    Gültige Werte: 0 ... 255

  - *aufeinanderfolgend verlorene Pakete*: Geben Sie hier den Schwellwert für die aufeinanderfolgend verlorenen Pakete ein. Es wird gezählt, wie viele Pakete aufeinanderfolgend (ohne Unterbrechung durch fehlerfreie Pakete) verloren gegangen sind. Wenn der gezählte Wert größer als der angegebene Wert ist, liegt eine Schwellwertüberschreitung vor.
    Standardwert: 2
    Gültige Werte: 0 ... 255

  - *aufeinanderfolgend verarbeitete Pakete*: Geben Sie hier den Schwellwert der aufeinanderfolgend verarbeiteten Pakete ein. Es wird gezählt, wie viele Pakete hintereinander fehlerfrei waren, ohne durch verlorene Pakete unterbrochen zu sein. Wenn der gezählte Wert kleiner als der angegebene Wert ist liegt eine Schwellwertüberschreitung vor.
    Standardwert: 8
    Gültige Werte: 0 ... 255

- *Schwellwerte für Nicht-Komprimierungs-Codec*: Geben Sie hier die gewünschte Anzahl in Paketen der Schwellwerte für die Nicht-Komprimierungs-Codec ein. Folgende Möglichkeiten stehen Ihnen zur Auswahl:

  - *verlorene Pakete (pro 1000 Pakete)*: Erklärung siehe *Schwellwerte für Komprimierungs-Codec*.

  - *aufeinanderfolgend verlorene Pakete*: Erklärung siehe *Schwellwerte für Komprimierungs-Codec*.

- *aufeinanderfolgend verarbeitete Pakete*: Erklärung siehe *Schwellwerte für Komprimierungs-Codec*.

Erklärung und Verwendung von Komprimierungs- und Nicht-Komprimierungs-Codec:

Codec	Audio-Mode	Verwendung
Hohe Qualität bevorzugt	Unkomprimierte Sprachübertragung.	Unkomprimierte Sprachübertragung verwenden. Geeignet für breitbandige Intranetverbindungen.
Niedrige Bandbreite bevorzugt	Bevorzugt komprimierte Sprachübertragung verwenden.	Geeignet für Verbindungen mit unterschiedlicher Bandbreite.
Nur geringe Bandbreite	Ausschließlich komprimierte Sprachübertragung verwenden.	Geeignet für Verbindungen mit geringer Bandbreite.

Tabelle 1 Codec - Betriebsarten

Klicken Sie auf *Übernehmen* und im Bestätigungsdialog auf *OK* (neuen Konfigurationszustand dauerhaft speichern mit Sichern-Symbol im Steuerbereich). Der Dialog *Quality of Service Data Collection* wird wieder angezeigt.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen sind OpenScape Access 500i/a bzw. OpenScape 4000 SoftGate neu zu starten.
- *Rückgängig:* Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt.

3.8 Picture CLIP

WBM-Pfad

WBM **>** *Konfiguration* **>** *Picture CLIP*

Das Menü *Picture CLIP* wird geöffnet:

Menü *Diverse*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

Einstellungen
Test

Leistungsmerkmalbeschreibung

Das Leistungsmerkmal Picture CLIP ermöglicht das Konfigurieren der Parameter für den direkten und indirekten Zugriff auf Telefonbilder, die entweder im LDAP-Verzeichnis (direkter Zugriff) oder auf einem externen Directory Server (indirekter Zugriff) gespeichert sind.

Das Leistungsmerkmal “Picture CLIP” bietet die Möglichkeit, während der Verbindung zentral gespeicherte Kontaktdaten (Name und Bild) des Gesprächspartners im Display eines IP-Telefons anzuzeigen.

Für die Anzeige zentral gespeicherter Kontaktdaten fordern die OpenStage-Telefone die Daten von einem OpenScape 4000 SoftGate an. Dieser leitet die Anfrage an einen zentralen Verzeichnisserver weiter, ruft die Daten ab und stellt sie anschließend den OpenStage-Telefonen zur Verfügung.

Das Anzeigeformat (Position, Darstellung, Größe usw.) der Kontaktdaten entspricht dem beim Nachschlagen im lokalen Telefonbuch verwendeten Anzeigeformat, da in beiden Fällen derselbe Mechanismus genutzt wird.

Der Verzeichnisserver wird für alle Nummern abgefragt. Wenn auf dem LDAP-Verzeichnisserver ein Eintrag zu der Nummer gefunden wird, werden der Name und das Bild vom Verzeichnisserver angezeigt. Wenn auf dem Verzeichnisserver kein Eintrag zu der Nummer gespeichert ist, wird der Name aus dem lokalen Telefonbuch angezeigt.

HINWEIS: Bei einem vom Telefon abgehendem Ruf wird das Bild für den angerufenen Kontakt nicht angezeigt, da hier das Ruf-Symbol (z. B. Frei-, Besetzt-, Umleitungs-Symbol, etc.) dargestellt werden muss.

Derzeit werden zwei verschiedene Modi für den Abruf von Bildern unterstützt:

Direkter Abruf von Bildern

Vorbedingungen:

- Direkter Abruf von Bildern konfiguriert.
- Kontaktdaten mit Bild auf dem LDAP-Server gespeichert.

=> Dem Benutzer werden der Name und das Bild des Gesprächspartners aus dem LDAP-Verzeichniseintrag angezeigt.

Das OpenStage-Telefon führt einen sogenannten Lookup (Nachschlagen) zum OpenScape 4000 SoftGate durch. Das OpenScape 4000 SoftGate leitet die Anfrage weiter zum LDAP-Server und empfängt Name und Bild der abgefragten Rufnummer. Name und Bild werden dann zusammen vom OpenScape 4000 SoftGate zum OpenStage-Telefon weitergeleitet und im Display angezeigt.

Indirekter Abruf von Bildern

Vorbedingungen:

- Indirekter Abruf von Bildern konfiguriert.
- Kontaktdaten auf dem LDAP-Server gespeichert, mit gültigem Verweis auf ein Bild, das auf einem anderen Webserver gespeichert ist.

=> Dem Benutzer werden der Name des Gesprächspartners aus dem LDAP-Verzeichniseintrag und das auf dem Webserver gespeicherte Bild angezeigt.

Das OpenStage-Telefon führt einen sogenannten Lookup (Nachschlagen) zum OpenScape 4000 SoftGate durch. Das OpenScape 4000 SoftGate leitet die Anfrage weiter zum LDAP-Server und empfängt Name und eine URL des Webservers mit zugehöriger Photo-ID wo das Bild gespeichert ist. Im nächsten Schritt empfängt das OpenScape 4000 SoftGate das Bild anhand der zuvor erhaltenen URL und Photo-ID. Name und Bild werden dann zusammen vom OpenScape 4000 SoftGate zum OpenStage-Telefon weitergeleitet und im Display angezeigt.

Picture CLIP – Serviceinformationen

- Dieses Leistungsmerkmal wird für OpenScape 4000 SoftGate und OpenScape Access 500 unterstützt.
- Wenn kein Bild verfügbar ist, werden nur der Name und die Nummer aus dem LDAP-Verzeichniseintrag angezeigt.
- Wenn der LDAP-Verzeichnisserver nicht erreichbar ist, wird nach Ablauf einer bestimmten Zeitspanne der PBX-Name angezeigt.
- Dieses Leistungsmerkmal wird nur von OpenStage 60 HFA und OpenStage 80 HFA unterstützt.
- Die OpenStage-Telefone müssen das OpenScape 4000 SoftGate oder die OpenScape Access 500, welche für Picture CLIP konfiguriert ist, erreichen können. Die OpenStage-Telefone müssen also nicht zwingend auf dem jeweiligen OpenScape 4000 SoftGate oder OpenScape Access 500 eingerichtet sein.
- Die OpenStage-Telefone akzeptieren nur im jpg-Format codierte Bilder mit einer Größe von maximal 50 KB.

- Für die zentrale Speicherung der Kontaktdaten und Bilder wird ein LDAP-Verzeichnisserver benötigt. Für den indirekten Abruf von Bildern ist zusätzlich ein Webserver erforderlich.
- Die Kontaktdaten werden auf dem LDAP-Verzeichnisserver mit den per WBM im OpenScape 4000 SoftGate konfigurierten Schlüsseln gespeichert.
- Es wird empfohlen, Telefonnummern im vollqualifizierten Format mit Landeskennzahl und Ortskennzahl zu speichern (z.B. 4989700754321). Wenn die Rufnummern mit Trennzeichen wie Klammern, Bindestrichen oder Pluszeichen gespeichert werden (z. B. +49 (89) 7007-54321), muss der LDAP-Verzeichnisserver bei der Rufnummernabfrage Umsetzungsregeln anwenden. Das OpenStage-Telefon verwendet für eine LDAP-Abfrage reine Ziffernfolgen ohne Trennzeichen.
- Die Kontaktdaten des LDAP-Verzeichnisservers werden unter Umständen erst nach kurzer Verzögerung angezeigt, da eine sichere Verbindung über https zum OpenScape 4000 SoftGate aufgebaut werden muss. Während dieser Zeit könnte der im OpenScape 4000 System hinterlegte Displayeintrag kurz angezeigt werden. Im Modus des indirekten Abrufs ist ein weiterer Request/ Response-Zyklus erforderlich um das Bild abzurufen.

3.8.1 Einstellungen

WBM-Pfad

WBM **>** *Konfiguration* **>** *Picture CLIP > Einstellungen*

Der Dialog *Einstellungen für Picture CLIP* wird angezeigt.

Auswahl- und Eingabefelder

In diesem Dialog gibt es folgende Auswahl-/Eingabefelder:

Feld	Beschreibung
LDAP-Server-Einstellungen	
LDAP-Server URL	Die URL (einschließlich Protokoll und Port) für den Zugriff auf den Directory Server
User DN	LDAP-Account
Passwort	Passwort
LDAP-Basisknoten	Knoten, unter dem die Kontaktdaten gespeichert sind
Suchen ab	Pfad, unter dem die Kontaktdaten gespeichert sind
LDAP-Schlüssel	
Büronummer	Rufnummer des Bürotelefons
Handynummer	Rufnummer des Mobiltelefons
Weitere Büronummer	Alternative Rufnummer des Bürotelefons

Feld	Beschreibung
Vornamen	Vorname(n) des Mitarbeiters
Nachname	Nachname des Mitarbeiters
Direkter Bild-Zugriff	
Bild	Bezeichnung (Schlüssel) unter der/dem das Bild gespeichert ist
Indirekter Bild-Zugriff	
Bilddateiname	Dateiname des Bildes (für indirekten Bildzugriff, kann bei direktem Bildzugriff leer bleiben)
URL des Bilderver-zeichnisses	URL des Verzeichnisses, in dem die Bilder gespeichert sind (für indirekten Bildzugriff, kann bei direktem Bildzugriff leer bleiben)

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die Eingaben werden gespeichert. Zum Aktivieren der Änderungen sind OpenScape Access 500i/a bzw. OpenScape 4000 SoftGate neu zu starten.
- *Rückgängig:* Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt.

3.8.2 Test

Sie können testen, ob der LDAP-Server-Zugang korrekt konfiguriert ist.

WBM-Pfad

WBM **>** *Konfiguration* **>** *Picture CLIP > Test*

Der Dialog *Picture CLIP testen* wird angezeigt.

Vorgehen

1. Klicken Sie auf die Schaltfläche **In separatem Fenster öffnen**. Das Fenster „Telefonnummernsuche” wird angezeigt.
2. Geben Sie in das Eingabefeld „Telefonnummer” eine Rufnummer ein und klicken Sie auf **OK**.

   Wenn der LDAP-Server-Zugang korrekt konfiguriert ist und zu der Rufnummer im LDAP ein Eintrag existiert, wird am unteren Rand des Fensters ein „Ergebnis” angezeigt.

   Man kann den Nachnamen und Vornamen erkennen. Die Zeichen danach bedeuten, dass außerdem ein Bild vorhanden ist.

Wenn der LDAP-Server-Zugang falsch konfiguriert ist, wird eine eindeutige Fehlermeldung angezeigt, z. B. *Problem beim Verbinden mit dem LDAP-Server*.

4 Wartung

Das Modul *Wartung* stellt Funktionen für die Wartung und Administration der vHG 3575 zur Verfügung. Dazu gehören das Durchführen von Software-Updates, das Sichern der Konfiguration, das Arbeiten mit Protokolldateien, das Aktivieren von Trace-Profilen, das Erstellen eines Secure Trace, das Erstellen von Diagnosedateien und das Ermitteln von Status-Informationen über OpenScape 4000 SoftGate und H.323-Telefone.

WBM-Pfad

WBM **>** *Wartung*

Das Modul *Wartung* wird geöffnet.

Auswahlmöglichkeiten im Modul *Wartung*

SW-Update
Backup/Restore
Logs
Trace
Secure Trace
Diagnose
Status-Information
Reboot / Shutdown OS

4.1 SW-Update

Im Menü *SW-Update* (SW: Software) werden Funktionen zum Anzeigen der Software-Version, für das Software-Update und für die Software-Aktivierung der vHG 3575 zur Verfügung gestellt.

WBM-Pfad

WBM **>** *Wartung* **>** *SW-Update*

Das Menü *SW-Update* wird geöffnet.

Menü *SW-Update*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

SW-Version anzeigen
LW-Update
LW-Aktivierung
OS-Update

4.1.1 SW-Version anzeigen

WBM-Pfad

WBM **>** *Wartung* **>** *SW-Update* **>** *SW-Version anzeigen*

Der Dialog *Softwareversion* wird angezeigt. Dieser Dialog enthält Details über die momentan installierten Software- und Hardwareversionen.

Angaben

Im Einzelnen werden folgende Angaben gemacht:

- ***System Version (PBX)***: Dieser Bereich zeigt die OpenScape 4000 Version unter:

  System Version

- ***Plattform Version***: Dieser Bereich zeigt an, auf welcher Hardware der vHG 3575 läuft, z.B. OpenScape Access 500. Die Angaben dazu sind:

  Hardware, *Platform Deployment*, *Platform Version*, *Importierte Platform Version*, *OS-Update Status*

- ***SoftGate Version***: Dieser Bereich zeigt die installierten Software und Loadwareversionen an. Das sind:

  Softwareversion, *Loadwarename*, *Loadwarevariante*, *APS-Version*

- ***SoftGate Komponentenversionen***: Dieser Bereich zeigt die installierten SoftGate-Komponenten ihre Versionen. Das sind:

  IMS SVN Version, *SoftGate SVN Version*, *CLA Version*, *Soco-common Version*, *OpenSIPS Version*

- ***Zusätzliche Packageversionen***: Dieser Bereich zeigt zusätzlich benötigte Software und ihre Versionen. Das ist:

  Java Version

4.1.2 LW-Update

WBM-Pfad

WBM **>** *Wartung* **>** *SW-Update* **>** *LW-Update*

Der Dialog *Loadwareaktualisierung* wird angezeigt. In diesem Dialog kann die vHG 3575-Applikation geladen werden.

Eingabefeld

In diesem Dialog gibt es das folgende Eingabefeld:

- *Dateiname:* In dieses Eingabefeld sind der Pfad und der Name der Datei einzugeben, welche die aktuelle Software enthält. Über die Schaltfläche *Durchsuchen* kann die Datei auch ausgewählt werden.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Laden:* Die angegebene Datei wird geladen.
- *Rückgängig:* Der eingegebene Pfad und der Dateiname werden gelöscht.

Vorgehen

Führen Sie zum Laden der vHG 3575-Applikation die folgenden Schritte durch:

1. Geben Sie den Pfad und den Namen der Datei ein, welche die aktuelle Software enthält oder wählen Sie über die Schaltfläche *Durchsuchen* die Datei aus.
2. Klicken Sie auf die Schaltfläche *Laden*. Die Software wird geladen. Nach dem Laden wird die nächste WBM-Seite automatisch eingeblendet.

4.1.3 LW-Aktivierung

WBM-Pfad

WBM **>** *Wartung* **>** *SW-Update* **>** *LW-Aktivierung*

Der Dialog *Loadwareaktivierung* wird angezeigt. In diesem Dialog kann die geladene vHG 3575-Applikation entweder sofort oder zeitgesteuert – zu einem bestimmten Zeitpunkt oder nach einer bestimmten Dauer – aktiviert werden.

Angaben

In diesem Dialog gibt es die folgenden Angaben:

- *Softwareversion*: Zeigt die Softwareversion der im Dialog *Softwareaktualisierung* geladenen vHG 3575-Applikation an.
- *Start der Aktion am*: Die Aktivierung der geladenen vHG 3575-Applikation soll zu einem bestimmten Zeitpunkt stattfinden. Der Tag dieses Zeitpunktes ist entweder über die Auswahlfelder oder über die Schaltfläche *Kalender* festlegbar.
- *Start der Aktion in*: Die Aktivierung der geladenen vHG 3575-Applikation soll nach Ablauf einer bestimmten Zeitdauer stattfinden.
- *Aktion stoppen*: Eine bereits vorher gestartete Aktion für die zeitgesteuerte Aktivierung wird gestoppt.
- *Systemzeit*: Diese Zeit ist die lokale Zeit des OpenScape und die Bezugszeit für die zeitgesteuerte Aktivierung. Die Angaben sind nicht editierbar.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die geänderten Einstellungen werden gespeichert.
- *Rückgängig:* Die geänderten Einstellungen werden verworfen und auf den Defaultwert zurückgesetzt.
- *Sofort starten:* Die Aktivierung der vHG 3575-Applikation wird sofort gestartet.

Vorgehen für sofortige Aktivierung

Führen Sie zum sofortigen Aktivieren der geladenen Software die folgenden Schritte durch:

1. Klicken Sie auf die Schaltfläche *Sofort starten*. Die Software wird aktiviert.

Vorgehen für zeitgesteuerte Aktivierung

Führen Sie zum zeitgesteuerten Aktivieren der geladenen Software die folgenden Schritte durch:

1. Zeitpunkt oder Dauer festlegen:
   - Zeitpunkt, zu dem die Aktivierung gestartet werden soll: Aktivieren Sie den Radio-Button *Start der Aktion am* und geben Sie in den Auswahl- und Eingabefeldern *Tag*, *Monat*, *Jahr*, *STD:MM* den Zeitpunkt an. Die Schaltfläche *Kalender* kann dazu ebenfalls benutzt werden.
   - Dauer, nach der die Aktivierung gestartet werden soll: Aktivieren Sie den Radio-Button *Start der Aktion in* und geben Sie in den Eingabefeldern *Tagen* und *STD:MM* die Dauer an.
2. Klicken Sie auf die Schaltfläche *Übernehmen*. Die Änderungen werden gespeichert. Die Aktion für die zeitgesteuerte Aktivierung wird gestartet.

Vorgehen für Stoppen der zeitgesteuerten Aktivierung

Führen Sie zum Stoppen einer Aktion für die zeitgesteuerte Aktivierung die folgenden Schritte durch:

1. Aktivieren Sie den Radio-Button *Aktion stoppen*.
2. Klicken Sie auf die Schaltfläche *Übernehmen*. Die Aktion wird gestoppt.

4.1.4 OS-Update

WBM-Pfad

WBM **>** *Wartung* **>** *SW-Update* **>** *OS-Update*

Menü *OS-Update*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

OS-Update Einstellungen
OS-Update Aktionen

4.1.4.1 OS-Update Einstellungen

WBM-Pfad

WBM **>** *Wartung* **>** *SW-Update* **>** *OS-Update* **>** *OS-Update Einstellungen*

Der Dialog *OS-Update Einstellungen* wird angezeigt. In diesem Dialog können die Transferparameter vom zentralen Host für das Update des OS (Operating System) eingestellt werden. Diese Einstellungen können nur für einzelnstehende SoftGates vorgenommen werden.

WICHTIG: Diese Einstellungen sind mit OpenScape 4000 V7R1 bei einzelnstehenden SoftGates noch nicht möglich. Benutzen Sie stattdessen die Funktion „Remote Appliance Reinstall (RAR)".

P2P-Transferparameter vom zentralen Host (nur Standalone SoftGates)

- *Max. Downloadgeschwindigkeit beschränken*: Kontrollkästchen aktivieren/deaktivieren. Die maximale Downloadgeschwindigkeit für das Update des OS kann auf den Wert, der im darunterstehenden Eingabefeld festgelegt wird, beschränkt werden.
- *Max. Downloadgeschwindigkeit (KB/s)*: Eingabefeld für die maximale Downloadgeschwindigkeit in KByte je Sekunde

- *Max. Uploadgeschwindigkeit beschränken*: Kontrollkästchen aktivieren/ deaktivieren. Die maximale Uploadgeschwindigkeit für das Update des OS kann auf den Wert, der im darunterstehenden Eingabefeld festgelegt wird, beschränkt werden.
- *Max. Uploadgeschwindigkeit (KB/s)*: Eingabefeld für die maximale Uploadgeschwindigkeit in KByte je Sekunde

Schaltflächen:

- *Übernehmen*: Die Eingaben werden gespeichert.
- *Rückgängig*: Die Eingaben werden verworfen und auf den Defaultwert zurückgesetzt.

4.1.4.2 OS-Update Aktionen

WBM-Pfad

WBM **>** *Wartung* **>** *SW-Update* **>** *OS-Update* **>** *OS-Update Aktionen*

Der Dialog *OS-Update Aktionen* wird angezeigt. In diesem Dialog kann der Transfer vom zentralen Host für das Update des OS (Operating System) abgebrochen werden (nur für einzelnstehende SoftGates). Für survivable SoftGates kann das OS-Update aktiviert werden.

WICHTIG: Diese Einstellungen sind mit OpenScape 4000 V7R1 bei einzelnstehenden SoftGates noch nicht möglich. Benutzen Sie stattdessen die Funktion „Remote Appliance Reinstall (RAR)".

OS-Update Transfer vom zentralen Host (nur Standalone SoftGates)

Schaltfläche:

- *Transfer abbrechen*: Der Transfer der OS-Software wird abgebrochen.

OS-Update Aktivierung (nur Surv. SoftGates)

- *Platform Version*: Anzeige der OpenScape 4000 Version
- *Importierte Platform Version*: Anzeige der importierten OpenScape 4000 Version
- *OS-Update Status*: Anzeige, ob ein neues Update-Packet für das OS verfügbar ist.
- *SoftGate-LW aus dem Updatepaket verwenden (empfohlen)*: Aktivierbar/ Deaktivierbar.

Schaltfläche:

- *OS-Update aktivieren*: Das OS-Update für das survivable SoftGate aktivieren.

4.2 Backup/Restore

Im Menü *Backup/Restore* kann die Konfiguration und die Sicherheitskonfiguration der vHG 3575 lokal gesichert (exportiert) werden. Diese lokale Sicherung kann geladen (importiert) und anschließend aktiviert werden.

WBM-Pfad

WBM **>** *Wartung* **>** *Backup/Restore*

Das Menü *Backup/Restore* wird geöffnet.

Menü *Backup/Restore*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

Export Konfiguration
Export Sicherheitskonf.
Import Konfiguration
Import Sicherheitskonf.

4.2.1 Export Konfiguration

WBM-Pfad

WBM **>** *Wartung* **>** *Backup/Restore* **>** *Export Konfiguration*

Der Dialog *Konfiguration exportieren* wird angezeigt. In diesem Dialog kann die Konfiguration der vHG 3575 lokal gesichert (exportiert) werden.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Das Exportieren der Konfiguration wird gestartet.
- *Rückgängig:* Das Exportieren der Konfiguration wird abgebrochen.

Vorgehen

Führen Sie zum Exportieren der Konfiguration die folgenden Schritte durch:

1. Klicken Sie auf die Schaltfläche *Übernehmen*. Die Konfiguration wird in eine zip-Datei exportiert. Es erscheint ein Fenster *Dateidownload* mit einer Abfrage, ob die zip-Datei geöffnet oder gespeichert werden soll.
2. Klicken Sie auf die Schaltfläche *Speichern* und wählen Sie den gewünschten Ordner für die Datei aus. Klicken Sie dann auf die Schaltfläche *OK*. Die zip-Datei wird gespeichert.

4.2.2 Export Sicherheitskonf.

WBM-Pfad

WBM **>** *Wartung* **>** *Backup/Restore* **>** *Export Sicherheitskonf.*

Der Dialog *Sicherheitskonfiguration exportieren* wird angezeigt. In diesem Dialog kann die Sicherheitskonfiguration der vHG 3575 lokal gesichert (exportiert) werden.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Das Exportieren der Sicherheitskonfiguration wird gestartet.
- *Rückgängig:* Das Exportieren der Sicherheitskonfiguration wird abgebrochen.

Vorgehen

Führen Sie zum Exportieren der Sicherheitskonfiguration die folgenden Schritte durch:

1. Klicken Sie auf die Schaltfläche *Übernehmen*. Die Sicherheitskonfiguration wird in eine zip-Datei exportiert. Es erscheint ein Fenster *Dateidownload* mit einer Abfrage, ob die zip-Datei geöffnet oder gespeichert werden soll.
2. Klicken Sie auf die Schaltfläche *Speichern* und wählen Sie den gewünschten Ordner für die Datei aus. Klicken Sie dann auf die Schaltfläche *OK*. Die zip-Datei wird gespeichert.

4.2.3 Import Konfiguration

WBM-Pfad

WBM **>** *Wartung* **>** *Backup/Restore* **>** *Import Konfiguration*

Der Dialog *Konfiguration importieren* wird angezeigt. In diesem Dialog kann die zuvor lokal gesicherte Konfiguration der vHG 3575 wieder importiert werden.

Eingabefeld

In diesem Dialog gibt es das folgende Eingabefeld:

- *Dateiname:* In dieses Eingabefeld sind der Pfad und der Name der Datei einzugeben, welche die zu importierende Konfiguration enthält. Über die Schaltfläche *Durchsuchen* kann die Datei auch ausgewählt werden.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Laden:* Die angegebene Konfigurationsdatei wird geladen.

- *Rückgängig:* Der eingegebene Pfad und der Dateiname werden gelöscht.

Vorgehen

Führen Sie zum Importieren einer Konfigurationsdatei die folgenden Schritte durch:

1. Geben Sie den Pfad und den Namen der Konfigurationsdatei ein oder wählen Sie über die Schaltfläche *Durchsuchen* die Datei aus.
2. Klicken Sie auf die Schaltfläche *Laden*. Die Konfigurationsdatei wird geladen.

WICHTIG: Damit alle Konfigurationsänderungen wirksam werden, muss vHG 3575 neu gestartet werden.

4.2.4 Import Sicherheitskonf.

WBM-Pfad

WBM **>** *Wartung* **>** *Backup/Restore* **>** *Import Sicherheitskonf.*

Der Dialog *Sicherheitskonfiguration importieren* wird angezeigt. In diesem Dialog kann die zuvor lokal gesicherte Sicherheitskonfiguration der vHG 3575 wieder importiert werden.

Eingabefeld

In diesem Dialog gibt es das folgende Eingabefeld:

- *Dateiname:* In dieses Eingabefeld sind der Pfad und der Name der Datei einzugeben, welche die zu importierende Sicherheitskonfiguration enthält. Über die Schaltfläche *Durchsuchen* kann die Datei auch ausgewählt werden.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Laden:* Die angegebene Datei wird geladen.
- *Rückgängig:* Der eingegebene Pfad und der Dateiname werden gelöscht.

Vorgehen

Führen Sie zum Importieren einer Sicherheitskonfiguration die folgenden Schritte durch:

1. Geben Sie den Pfad und den Namen der Datei ein, welche die zu importierende Sicherheitskonfiguration enthält oder wählen Sie über die Schaltfläche *Durchsuchen* die Datei aus.
2. Klicken Sie auf die Schaltfläche *Laden*. Die Datei wird geladen.

WICHTIG: Damit alle Konfigurationsänderungen wirksam werden, muss vHG 3575 neu gestartet werden.

4.3 Logs

Im Menü *Logs* können für Diagnosezwecke die Protokolldateien in eine zip-Datei exportiert werden. Zum Anlegen neuer Protokolldateien ist das Löschen der alten, d.h. exportierten, Protokolldateien möglich.

WBM-Pfad

WBM **>** *Wartung* **>** *Logs*

Das Menü *Logs* wird geöffnet.

Menü *Logs*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

Logs exportieren
Logs löschen

4.3.1 Logs exportieren

WBM-Pfad

WBM **>** *Wartung* **>** *Logs* **>** *Logs exportieren*

Der Dialog *Protokolldateien exportieren* wird angezeigt. In diesem Dialog können die Protokolldateien der vHG 3575 lokal gesichert (exportiert) werden.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Exportieren:* Die über die Kontrollkästchen ausgewählten Protokolldateien werden lokal gesichert (exportiert).

Vorgehen

Führen Sie zum Exportieren von Protokolldateien die folgenden Schritte durch:

1. Klicken Sie auf die Schaltfläche *Exportieren*. Die Protokolldateien werden in eine zip-Datei exportiert. Es erscheint eine Abfrage, ob die zip-Datei geöffnet oder gespeichert werden soll.
2. Klicken Sie auf die Schaltfläche *Speichern* und wählen Sie den gewünschten Ordner für die Datei aus. Klicken Sie dann auf die Schaltfläche *OK*. Die zip-Datei wird gespeichert.

4.3.2 Logs löschen

WBM-Pfad

WBM **>** *Wartung* **>** *Logs* **>** *Logs löschen*

Der Dialog *Protokolldateien löschen* wird angezeigt. In diesem Dialog können die aufgelisteten Protokolldateien einzeln oder insgesamt markiert und gelöscht werden.

Kontrollkästchen

In diesem Dialog gibt es die folgenden Kontrollkästchen:

- *Soco*, *JLM*, *IMS*, *SPA, Status Collector*, *Update*, *Backtrace*, *Heap-Dump*, *Corelogs*, *Garbage collection*, *Gateway (vHG) Logs, LS-DCL, Load-Balancer*, *DHCP*
- *Alles:* Es werden alle Protokoll-(Diagnose)dateien markiert.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Löschen:* Alle über die Kontrollkästchen markierten Protokolldateien werden gelöscht.
- *Rückgängig:* Die geänderten Einstellungen werden verworfen und auf den Defaultwert zurückgesetzt.

Vorgehen

Führen Sie zum Löschen von Protokolldateien die folgenden Schritte durch:

1. Aktivieren Sie die Kontrollkästchen derjenigen Protokolldateien, die Sie löschen möchten.
2. Klicken Sie auf die Schaltfläche *Löschen*. Die markierten Protokolldateien werden gelöscht.

4.4 Trace

Unter *Trace* können Trace-Profile aktiviert werden.

WBM-Pfad

WBM **>** *Wartung* **>** *Trace*

Das Menü *Trace* wird geöffnet.

Menü *Trace*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

Profile

4.4.1 Profile

HINWEIS: Diese Funktion darf nur von Entwicklern benutzt werden. Für die Standard-Analyse werden die Funktionen im Dialog *Diagnose-Dateien* empfohlen (siehe Abschnitt 4.7.2, “Diagnose-Dateien”).

WBM-Pfad

WBM **>** *Wartung* **>** *Trace* **>** *Profile*

Der Dialog *Trace-Profile-Konfiguration editieren* wird angezeigt. In diesem Dialog können Trace-Profile für eine detaillierte Analyse der vHG 3575 aktiviert werden. Durch jedes Trace-Profil werden spezielle Informationen aufgezeichnet.

Trace-Profile

Durch Aktivierung der hier genannten Trace-Profile können die folgenden Probleme untersucht werden:

- *acw-cc*: Entwickler-spezifisch
- *acw-cc*: Entwickler-spezifisch
- *cg*: Entwickler-spezifisch
- *dataloading*: Entwickler-spezifisch
- *dcl2*: Entwickler-spezifisch
- *debug-all*: Entwickler-spezifisch
- *dmc-detail*: Entwickler-spezifisch
- *heap-diag*: Entwickler-spezifisch

- *hfa-call*: Wird verwendet bei Problemen mit der Signalisierung von HFA-Verbindungen und dem An- und Abmelden der HFA-Endgeräte.
- *hfa-reg*: Wird verwendet bei Problemen mit der Registrierung der HFA-Endgeräte, z. B. bei fehlerhaften Anzeigen in den Endgeräte-Displays.
- *hsr*: Wird verwendet bei Problemen mit der Verbindung zwischen SoftGate und Host.
- *hsr-message-dump*: Entwickler-spezifisch. Beeinträchtigt die Leistung des Systems!
- *ipconfig*: Entwickler-spezifisch
- *ipv6*: Wird verwendet, wenn Probleme bei der Vernetzung über IP V6 bestehen.
- *licensing*: Wird verwendet bei Problemen mit der SoftGate-Lizenzierung.
- *maintenance*: Entwickler-spezifisch
- *mmx*: Entwickler-spezifisch
- *osa*: Trace-Profil für OpenScape Access
- *osa-clock*: Trace-Profil für OpenScape Access
- *osa-light*: Trace-Profil für OpenScape Access
- *osa-trace*: Trace-Profil für OpenScape Access
- *payload*: Wird verwendet bei Problemen mit der Sprachdurchschaltung (wie *payload-light*). Beeinträchtigt die Leistung des Systems! Aufgrund der Erzeugung umfangreicher Trace-Ausgaben darf dieses Profil nicht bei hoher Systemlast aktiviert werden.
- *payload-light*: Wird verwendet bei Problemen mit der Sprachdurchschaltung. Kann bei erhöhter Systemlast aktiviert werden. Siehe auch Absatz „payload“.
- *payload-native*: Entwickler-spezifisch
- *qdc*: Entwickler-spezifisch
- *reconnect*: Entwickler-spezifisch
- *rrt*: Entwickler-spezifisch
- *scc*: Wird verwendet bei allgemeinen Payload-Problemen, bei Konferenz-Verbindungen und bei IPDA-Verbindungen.
- *sigsurv*: Entwickler-spezifisch
- *sip*: Nach Aktivierung dieses Trace-Profils werden die Trace-Meldungen der vHG 3575, die im lokalen WBM der vHG 3575 konfiguriert wurden, in die SoftGate-Protokolldatei übernommen. Gleichzeitig werden die SIP-relevanten scc-Traces aufgezeichnet.

- *siux*: Entwickler-spezifisch
- *slc*: Entwickler-spezifisch
- *startup*: Wird verwendet bei Hochlaufproblemen des SoftGates und der virtuellen Baugruppen.
- *sysinfo*: Entwickler-spezifisch
- *system*: Dieses Traceprofil ist immer aktiviert und kann nicht ausgeschaltet werden.
- *telnumlookup*: Entwickler-spezifisch
- *thread-profiling*: Entwickler-spezifisch
- *vSlma*: Entwickler-spezifisch
- *vTmom*: Entwickler-spezifisch
- *wbm*: Entwickler-spezifisch

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die Einstellungen der aktivierten/deaktivierten Kontrollkästchen werden gespeichert.
- *Rückgängig:* Die Einstellungen der aktivierten/deaktivierten Kontrollkästchen werden auf die Default-Einstellungen zurückgesetzt.

Vorgehen

Führen Sie zum Aktivieren von Trace-Profilen die folgenden Schritte durch:

1. Aktivieren Sie die Kontrollkästchen derjenigen Trace-Profile, die Sie für eine Analyse benötigen.
2. Klicken Sie auf die Schaltfläche *Übernehmen*. Die Einstellungen der aktivierten/deaktivierten Kontrollkästchen werden gespeichert.

4.5 Secure Trace

Ein Secure Trace dient zum Ermitteln von Störungen im Kommunikationssystem. Durch den Secure Trace werden Aufzeichnungen über verschlüsselte VoIP-Nutz- und Signalisierungsdatenströme vom und zum vHG 3575 angefertigt.

Der Secure Trace enthält verschlüsselte Aufzeichnungen. Diese Aufzeichnungen können vom Entwickler durch einen Schlüssel entschlüsselt werden.

WBM-Pfad

WBM **>** *Wartung* **>** *Secure Trace*

Das Menü *Secure Trace* wird geöffnet.

Menü *Secure Trace*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

Zertifikat importieren
Zertifikat anzeigen
Status
Trace starten
Trace stoppen

Prinzipieller Ablauf der Secure Trace-Erstellung

Zum Erstellen eines Secure Trace ist der folgende Ablauf einzuhalten:

1. Der Servicetechniker stellt ein Problem im Netzwerk des Kunden fest. In einer Besprechung mit dem Entwickler wird die Notwendigkeit erkannt, einen Secure Trace zu erzeugen.
2. Der Kunde wird von der Notwendigkeit informiert und muss bestätigen, dass er informiert wurde. Danach gibt der Kunde eine Bestellung zum Erzeugen eines Secure Trace auf, in der Beginn und Ende (mit Datum und Uhrzeit) der Überwachung genannt sind.
3. Die Entwicklung erstellt ein Schlüsselpaar, das aus dem öffentlichen Schlüssel und dem privaten Schlüssel besteht. Mit dem Schlüsselpaar kann nur ein einziger Secure Trace erstellt werden. Die Zertifikate werden folgendermaßen verwendet:
   - Das Zertifikat mit dem privaten Schlüssel ist streng geheim und kann nur von autorisierten Entwicklern benutzt werden (Whitelist).
   - Das Zertifikat mit dem öffentlichen Schlüssel wird an den Servicetechniker übergeben bzw. kann von der HiSat Homepage (https://hisat.global-intra.net/wiki/index.php/SecureTrace) heruntergeladen werden.

4. Der Servicetechniker informiert den Kunden über den Beginn der Trace-Aktivitäten. Der Kunde muss die betroffenen Teilnehmer informieren.

WICHTIG: Das Aufzeichnen von Gesprächen und Verbindungsdaten ist ein Straftatbestand, wenn die betroffenen Teilnehmer nicht informiert wurden!

---

5. Der Servicetechniker stellt den Gateways vHG 3575, für die ein Secure Trace zu erstellen ist, das Zertifikat zur Verfügung, siehe Abschnitt 4.5.1, “Zertifikat importieren”.
6. Der Servicetechniker aktiviert die Secure Trace-Funktion, siehe Abschnitt 4.5.4, “Trace starten”. Ein Secure Trace wird erstellt. Die Aktivierung und die spätere Deaktivierung (Abschnitt 4.5.5, “Trace stoppen”) werden von den beteiligten Kommunikationssystemen protokolliert.
7. Nachdem der Secure Trace erstellt wurde, wird der Kunde über das Ende der Trace-Aktivitäten informiert. Der Servicetechniker entfernt das Zertifikat vom System.
8. Der Secure Trace wird dem Entwickler zur Verfügung gestellt.
9. Der Entwickler entschlüsselt den Secure Trace, indem er den privaten Schlüssel anwendet. Danach analysiert er die entschlüsselten Aufzeichnungen.
10. Nach dem Ende der Analyse müssen alle relevanten Materialien und Daten auf eine sichere Art und Weise zerstört werden. Dies beinhaltet auch das Zerstören des privaten Schlüssels, damit eine eventuell angefertigte unerlaubte Kopie des Secure Trace nicht mehr entschlüsselt werden kann.

4.5.1 Zertifikat importieren

WBM-Pfad

WBM **>** *Wartung* **>** *Secure Trace* **>** *Zertifikat importieren*

Der Dialog *Laden des Secure Trace Zertifikats über HTTP* wird angezeigt. In diesem Dialog kann ein Secure Trace-Zertifikat importiert werden. Dieses Zertifikat ist die Voraussetzung dafür, dass ein Secure Trace erstellt werden kann. Der Servicetechniker bekommt es vom Entwickler. Es enthält den öffentlichen Schlüssel und muss im PEM- oder im binären Format vorliegen. Das Zertifikat ist maximal einen Monat gültig.

Eingabefeld

Dieser Dialog enthält das folgende Eingabefeld:

- *Datei mit dem Zertifikat (PEM- oder Binär-Format)*: In dieses Eingabefeld sind der Pfad und der Name der Datei, die das Zertifikat enthält, einzugeben. Über die Schaltfläche *Durchsuchen* kann die Datei auch ausgewählt werden.

Schaltflächen

Dieser Dialog enthält die folgenden Schaltflächen:

- *Fingerabdruck des Zertifikats anzeigen*: Durch Prüfen des Fingerabdrucks kann festgestellt werden, ob ein unverändertes Zertifikat vorliegt oder ob es verändert wurde.
- *Zertifikat aus Datei importieren*: Das Zertifikat wird aus der im oben genannten Eingabefeld angegebenen Datei importiert.

Vorgehen

Führen Sie zum Importieren des Zertifikats die folgenden Schritte durch:

1. Wählen Sie: *WBM* **>** *Wartung* **>** *Secure Trace* **>** *Zertifikat importieren.* Der Dialog *Laden des Secure Trace Zertifikats über HTTP* wird angezeigt.
2. Wählen Sie über die Schaltfläche *Durchsuchen* die Datei aus, die das Zertifikat enthält und bestätigen Sie mit *Öffnen*. Die Datei wird geladen.
3. Klicken Sie auf *Fingerabdruck des Zertifikats anzeigen*. Ein Fenster mit dem Fingerabdruck des zu importierenden Zertifikats wird angezeigt:
   a) Prüfen Sie den Fingerabdruck (hexadezimale Zahl). Wenn ein Zertifikat verändert wurde, ändert sich immer der Fingerabdruck. Nur ein unveränderter Fingerabdruck ist eine Gewähr für ein unverändertes Zertifikat. Sind die beiden Fingerabdrücke nicht identisch, dann liegt wahrscheinlich ein Angriffsversuch vor. In diesem Fall darf der Schlüssel nicht mehr verwendet werden; darüber hinaus sind die festgelegten Maßnahmen zu ergreifen.
   b) Klicken Sie auf *OK*, um das Fenster mit dem Fingerabdruck zu schließen.
4. Klicken Sie auf *Zertifikat aus Datei importieren*, wenn Sie mit der Prüfung des Fingerabdrucks zufrieden sind. Importieren Sie das Zertifikat nicht, falls der Fingerabdruck nicht Ihren Erwartungen entspricht.

Das Erstellen des Secure Trace ist nun möglich.

4.5.2 Zertifikat anzeigen

WBM-Pfad

WBM **>** *Wartung* **>** *Secure Trace* **>** *Zertifikat anzeigen*

Der Dialog *Zertifikatsinformationen* wird angezeigt. In diesem Dialog kann das Secure Trace-Zertifikat angezeigt werden, z. B. um es zu überprüfen.

Angezeigte Daten

Es werden die folgenden Daten aus dem Zertifikat angezeigt:

- Allgemeine Daten: *Name des Zertifikats*, *Zertifikatstyp*, *Seriennummer des Zertifikats*, *Seriennummer des Zertifikats (hex)*, *Signatur-Algorithmus-Typ*, *Beginn der Zertifikatsgültigkeit (GMT)*, *Ende der Zertifikatsgültigkeit (GMT)*, *CRL-Verteilungspunkt*
- *Ausgestellt durch CA*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name (CN)*
- *Antragsteller*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name (CN)*
- *Alternativer Antragstellername*
- *Daten des öffentl. Schlüssels*: *Länge des öffentl. Schlüssels*, *Öffentlicher Schlüssel*, *Fingerabdruck*

4.5.3 Status

WBM-Pfad

WBM **>** *Wartung* **>** *Secure Trace* **>** *Status*

Der Dialog *Secure Trace Status* wird angezeigt. In diesem Dialog können Sie feststellen, ob gerade ein Secure Trace erstellt wird.

Angezeigte Daten

Es werden die folgenden Daten angezeigt:

- *Secure Trace aktiviert*: Diese Zeile zeigt an, ob gerade ein Secure Trace erstellt wird.
- *Automatischer Deaktivierungszeitpunkt*: Diese Zeile zeigt an, wann der Secure Trace voraussichtlich erstellt ist und die Secure Trace-Funktion automatisch deaktiviert wird.
- *Secure Trace für folgende Protokolle*: Diese Zeile zeigt an, für welche Protokolle der Secure Trace erstellt wird. Das kann sein: Media Server (SRTP).

4.5.4 Trace starten

WBM-Pfad

WBM **>** *Wartung* **>** *Secure Trace* **>** *Trace starten*

Der Dialog *Secure Trace einschalten* wird angezeigt. In diesem Dialog kann der Secure Trace gestartet werden. Dazu müssen die folgenden Voraussetzungen vorliegen:

- Der Secure Trace ist noch nicht aktiviert.

- Der Kunde hat die Erstellung des Secure Trace veranlasst und möchte seine *Secure Trace Aktivierungs-Passphrase* in das WBM eingeben.
- Sie haben einen öffentlichen Schlüssel vom Entwickler bekommen und in das WBM geladen.

Eingabefelder und Kontrollkästchen

- *Start Parameter*:
  - *Secure Trace Aktivierungs-Passphrase*: Um die Nutzung der Secure Trace-Funktion zu begrenzen, wird die Aktivierung durch eine besondere Passphrase, die nur der Kunde kennt, geschützt. Somit ist diese Passphrase der Schlüssel des Kunden und das Zertifikat der Schlüssel des Servicetechnikers. Beide Schlüssel sind notwendig, um die Secure Trace-Funktion zu aktivieren.

    Eine Passphrase ist ein aus mehreren Wörtern bestehendes Passwort mit einer maximalen Länge von 20 Zeichen.
  - *Dauer des Secure Trace (Min.)*: Das Eingeben der Dauer des Secure Trace (in Minuten) ist unbedingt erforderlich.
- *Secure Trace für folgende Protokolle*:
  - *MMX (PEP)*: Der Secure Trace für MMX wird erstellt. Das Protokoll PEP (Protocol Extension Protocol) erweitert HTTP für Applikationen wie z. B. HTTP-Clients, Server und Proxy-Server.
  - *MediaServer (SRTP)*: Der Secure Trace für MediaServer wird erstellt. Das Protokoll SRTP (Secure Real-Time Transport Protocol) dient der verschlüsselten Übertragung über IP-basierte Netze und verwendet AES (Advanced Encryption Standard) für die Verschlüsselung.

Schaltfläche

In diesem Dialog gibt es die folgende Schaltfläche:

- *Secure Trace einschalten*: Der Secure Trace wird gestartet. Die oben genannten Voraussetzungen für das Starten des Secure Trace müssen vorliegen.

Vorgehen

Führen Sie zum Starten des Secure Trace die folgenden Schritte durch:

1. Prüfen Sie, ob die oben genannten Voraussetzungen vorliegen.
2. Wählen Sie: *WBM* **>** *Wartung* **>** *Secure Trace* **>** *Trace starten.* Der Dialog *Secure Trace einschalten* wird angezeigt.
3. Geben Sie im Bereich *Start Parameter* die *Secure Trace Aktivierungs-Passphrase* und die *Dauer des Secure Trace (Min.)* ein.

4. Aktivieren Sie das Protokoll *MediaServer (SRTP)*.
5. Klicken Sie auf die Schaltfläche *Secure Trace einschalten*. Der Secure Trace wird für die angegebene Zeitdauer erstellt.

4.5.5 Trace stoppen

WBM-Pfad

WBM **>** *Wartung* **>** *Secure Trace* **>** *Trace stoppen*

Der Dialog *Secure Trace beenden* wird angezeigt. In diesem Dialog kann ein laufender Secure Trace gestoppt werden, wenn die unter *Trace starten* festgelegte Zeitdauer noch nicht abgelaufen ist.

Schaltfläche

In diesem Dialog gibt es die folgende Schaltfläche:

- *Secure Trace beenden*: Der Secure Trace wird gestoppt.

4.6 DLS Client

Der DLS-Client dient der Administration von PKI-Daten und der QDC-Konfiguration (DLS: **D**ep**l**oyment **S**ervice oder **D**eployment- und **L**icencing **S**erver, PKI: **P**ublic **K**ey **I**nfrastructure, QDC: **Q**uality of Service **D**ata **C**ollection).

WBM-Pfad

WBM **>** *Wartung* **>** *DLS Client*

Das Menü *DLS Client* wird geöffnet.

Menü *DLS Client*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

DLS Einstellungen
PIN Eingabe
Bootstrapping zurücksetzen
DLS kontaktieren

Bootstrapping

Durch das Bootstrapping soll eine auf Zertifikaten basierende zuverlässige SSL-Verbindung zwischen DLS-Server und DLS-Client aufgebaut werden.

Ausgehend von einer Verbindungsanfrage des DLS-Clients an einen DLS-Server sowie der darauffolgenden Antwort –also einer noch unzuverlässigen Verbindung–, wird über die wechselseitige Authentifizierung und den Austausch von Zertifikaten eine zuverlässige Verbindung aufgebaut (d.h. Bootstrapping = ein einfaches System entwickelt sich zu einem komplexen System aus sich selbst heraus).

Da sich auf die Verbindungsanfrage des DLS-Clients anstatt des gewollten DLS-Servers auch ein anderer DLS-Server melden könnte, um die gewünschte Verbindung an sich zu ziehen, sind Sicherungsmaßnahmen notwendig. Mittels AMO kann der DLS-Server (d.h. dessen IP-Adresse und Port) administriert werden, den der DLS-Client kontaktieren soll.

Es wird empfohlen, den DLS-Client gegenüber dem DLS-Server durch Eingeben einer Bootstrap-PIN am WBM des vHG 3575, die zuvor vom DLS-Server per Zufall generiert wurde, zu autorisieren. Die Autorisierung des DLS-Clients kann auch mit einer nicht einzugebenden systeminternen Standard-PIN erfolgen, oder auf die Autorisierung mittels PIN kann auch ganz verzichtet werden. Diese beiden Möglichkeiten werden jedoch nicht empfohlen.

Nach dem Herstellen der zuverlässigen Verbindung werden die Zertifikate ausgetauscht, s.u.

Zertifikatsgenerierung und -verteilung für die Kommunikation zwischen DLS-Client und DLS-Server:

Alle Zertifikate und privaten Schlüssel für die verschlüsselte Kommunikation zwischen DLS-Client und DLS-Server werden durch eine selbst-signierende Zertifizierungsstelle (CA) des DLS-Servers erzeugt und durch den DLS-Server während des Bootstrappings zum DLS-Client gesendet.

Die vom DLS-Server zum DLS-Client gesendete PKCS#12-Datei enthält das DLSC Client-Zertifikat, den darin enthaltenen privaten Schlüssel und das Zertifikat der Zertifizierungsstelle des DLS-Servers (DLSC CA-Zertifikat). Der DLS-Server kann alle von ihm gelieferten Zertifikate zurücklesen, jedoch nicht den privaten Schlüssel.

Zertifikatsgenerierung und -verteilung für die sichere Verbindung des WBM zum DLS-Server:

Der Administrator sendet manuell das von der Kunden PKI-Zertifizierungsstelle erstellte WBM-Zertifikat, das den privaten Schlüssel enthält, zum OpenScape 4000 Assistant. Der OpenScape 4000 Assistant sendet dann automatisch sein WBM-Zertifikat zu allen CGWs. Mit diesem Zertifikat weist sich dann der DLS-Client gegenüber dem DLS-Server aus.

4.6.1 DLS Einstellungen

Außer dem automatischen Registrieren des DLS-Client am DLS-Server mittels der ContactMe-Antwort kann der DLS-Client auch manuell registriert werden. Dafür müssen Ihnen vom DLS-Server die IP-Adresse und der Port für den Bootstrapping-Modus bekannt sein. Die IP-Adresse und der Port des DLS-Servers können mittels AMO konfiguriert werden. Diese Änderung wird erst nach einem Neustart des vHG 3575 wirksam.

Nach Setzen von IP-Adresse und Port des DLS-Servers erfolgt beim Neustart (und jedem weiteren Neustart) ein einmaliger Versuch, durch Senden einer Verbindungsanfrage das Bootstrapping einzuleiten.

Unter dem Menüpunkt *DLS kontaktieren* können manuell weitere Verbindungsversuche eingeleitet werden. Falls noch kein Bootstrapping durchgeführt wurde, wird dies dabei automatisch eingeleitet, andernfalls wird lediglich geprüft, ob der DLS erreichbar ist.

WBM-Pfad

WBM **>** *Wartung* **>** *DLS Client* **>** *DLS Einstellungen*

Der Dialog *DLS Client Grundeinstellung ändern* wird geöffnet.

Eingabefeld

Im Bereich *Aktuelle DLS Client Grundeinstellung* gibt es folgendes Eingabefeld:

- *Zeitintervall für ContactMe-Antwort*: Zeit, die der DLS-Client nach Absenden seiner Verbindungsanfrage wartet, um die ContactMe-Antwort vom DLS-Server zu erhalten. Die Wartezeit muss begrenzt sein, damit ContactMe-Antworten von ungewollten DLS-Servern nicht empfangen werden können.

Anzeigen

In diesem Dialog gibt es die folgenden Anzeigen:

- *Aktuelle DLS Client Grundeinstellung*:

  - *PIN für DLS-Bootstrapping erforderlich*: Die PIN kann unter dem Menüpunkt *PIN Eingabe* eingegeben werden.
    Ja: Es wurde eine PIN eingegeben.
    Nein: es wurde keine PIN eingegeben.
  - *Sichere Kommunikation mit DLS-Server*: *Aktiviert* oder *Deaktiviert*

- *Aktuelle DLS Client Server Einstellung*:
  - *IP-Adresse des DLS-Servers*: IP-Adresse des DLS-Servers für den Bootstrapping-Modus kann mittels AMO konfiguriert werden. Ein Neustart des vHG 3575 ist erforderlich.
  - *Port des DLS-Servers*: Port des DLS-Servers für den Bootstrapping-Modus kann mittels AMO konfiguriert werden. Ein Neustart des vHG 3575 ist erforderlich.
  - *Port für sichere Verbindung zum DLS-Server*: Port des vHG 3575 für eine sichere Verbindung zum DLS-Server

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die geänderten Einstellungen werden gespeichert.
- *Rückgängig:* Die geänderten Einstellungen werden verworfen und auf den Defaultwert zurückgesetzt.

4.6.2 PIN Eingabe

WBM-Pfad

WBM **>** *Wartung* **>** *DLS Client* **>** *PIN Eingabe*

Der Dialog *Eingabe der Bootstrap PIN* wird geöffnet. In diesem Dialog kann die vom DLS-Server per Zufall generierte Bootstrap PIN eingegeben werden.

Eingabefeld

In diesem Dialog gibt es folgendes Eingabefeld:

- *Bootstrap PIN*: Wenn in dieses Eingabefeld eine PIN eingegeben und durch Klicken auf *Übernehmen* gespeichert wurde, wird im Dialog *DLS Client Grundeinstellung ändern* (Menüpunkt *DLS Einstellungen*) angezeigt, dass für das DLS-Bootstrapping eine PIN erforderlich ist.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die geänderten Einstellungen werden gespeichert.

- *Rückgängig:* Die geänderten Einstellungen werden verworfen und auf den Defaultwert zurückgesetzt.

4.6.3 Bootstrapping zurücksetzen

WBM-Pfad

WBM **>** *Wartung* **>** *DLS Client* **>** *Bootstrapping zurücksetzen*

Der Dialog *DLS Client Bootstrapping zurücksetzen* wird geöffnet.

Schaltfläche

In diesem Dialog gibt es die folgende Schaltfläche:

- *Bootstrapping zurücksetzen*: Das Bootstrapping des DLS-Clients wird zurückgesetzt.

4.6.4 DLS kontaktieren

Unter dem Menüpunkt *DLS kontaktieren* können manuell weitere Verbindungsversuche zum DLS-Server eingeleitet werden. Falls noch kein Bootstrapping durchgeführt wurde, wird dies dabei automatisch eingeleitet, andernfalls wird lediglich geprüft, ob der DLS erreichbar ist.

WBM-Pfad

WBM **>** *Wartung* **>** *DLS Client* **>** *DLS kontaktieren*

Der Dialog *DLS kontaktieren* wird geöffnet.

Menü *DLS kontaktieren*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

DLSC Client-Zertifikate
DLSC CA-Zertifikate

Dialog *DLS kontaktieren*

In diesem Dialog gibt es folgende Schaltfläche:

- *Kontaktieren*: Der DLS-Server wird kontaktiert, um zu überprüfen, ob er noch verfügbar ist.

4.6.4.1 DLSC Client-Zertifikate

Unter diesem Menüpunkt befinden sich die DLSC Client-Zertifikate mit dem privaten Schlüssel. Mit diesen Zertifikaten weist sich der DLS-Client gegenüber dem DLS-Server aus. Während des Bootstrapping-Modus bekommt der DLS-Client das Zertifikat vom DLS-Server.

WBM-Pfad

WBM **>** *Wartung* **>** *DLS Client* **>** *DLSC Client-Zertifikate*

Das Menü *DLSC Client-Zertifikate* wird geöffnet.

Menü *DLSC Client-Zertifikate*

Unter diesem Menüpunkt sind die einzelnen DLSC Client-Zertifikate auswählbar:

1. DLSC Client-Zertifikat

4.6.4.2 1. DLSC Client-Zertifikat

WBM-Pfad

WBM **>** *Wartung* **>** *DLS Client* **>** *DLSC Client-Zertifikate* **>** *1. DLSC Client-Zertifikat*

Der Dialog *Zertifikatsinformationen* wird geöffnet.

Angezeigte Daten

Es werden die folgenden Daten aus dem Zertifikat angezeigt:

- Allgemeine Daten: *Zertifikatstyp*, *Seriennummer des Zertifikats*, *Seriennummer des Zertifikats (hex)*, *Signatur-Algorithmus-Typ*, *Beginn der Zertifikatsgültigkeit (GMT)*, *Ende der Zertifikatsgültigkeit (GMT)*, *CRL-Verteilungspunkt*
- *Ausgestellt durch CA*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name (CN)*
- *Antragsteller*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name (CN)*
- *Alternativer Antragstellername*
- *Daten des öffentl. Schlüssels*: *Länge des öffentl. Schlüssels*, *Öffentlicher Schlüssel*, *Fingerabdruck*

4.6.4.3 DLSC CA-Zertifikate

Dieser Ordner enthält die vom DLS-Server während des Bootstrapping-Modus gelieferten DLSC CA-Zertifikate.

WBM-Pfad

WBM **>** *Wartung* **>** *DLS Client* **>** *DLSC CA-Zertifikate*

Das Menü *DLSC CA-Zertifikate* wird geöffnet.

Menü *DLSC CA-Zertifikate*

Unter diesem Menüpunkt sind die einzelnen DLSC Client-Zertifikate auswählbar:

„1. CA-Zertifikat“, „2. CA-Zertifikat“

4.6.4.4 „1. CA-Zertifikat“, „2. CA-Zertifikat“

WBM-Pfad

WBM **>** *Wartung* **>** *DLS Client* **>** *DLSC Client-Zertifikate* **>** *„1. CA-Zertifikat“, „2. CA-Zertifikat“*

Der Dialog *Zertifikatsinformationen* wird geöffnet.

Angezeigte Daten

Es werden die folgenden Daten aus dem Zertifikat angezeigt:

- Allgemeine Daten: *Zertifikatstyp*, *Seriennummer des Zertifikats*, *Signatur-Algorithmus-Typ*, *Beginn der Zertifikatsgültigkeit (GMT)*, *Ende der Zertifikatsgültigkeit (GMT)*, *CRL-Verteilungspunkt*
- *Ausgestellt durch CA*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name (CN)*
- *Antragsteller*: *Land (C)*, *Organisation (O)*, *Organisationseinheit (OU)*, *Allgemeiner Name (CN)*
- *Alternativer Antragstellername*
- *Daten des öffentl. Schlüssels*: *Länge des öffentl. Schlüssels*, *Öffentlicher Schlüssel*, *Fingerabdruck*

4.7 Diagnose

Unter *Diagnose* können Einstellungen zur Überwachung von IP-Verbindungen vorgenommen und Diagnose-Dateien erstellt werden.

WBM-Pfad

WBM **>** *Wartung* **>** *Diagnose*

Das Menü *Diagnose* wird geöffnet.

Menü *Diagnose*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

Diagnose-Funktionen
Diagnose-Dateien

4.7.1 Diagnose-Funktionen

WBM-Pfad

WBM **>** *Wartung* **>** *Diagnose* **>** *Diagnose-Funktionen*

Der Dialog *Diagnose-Funktionen* wird angezeigt. In diesem Dialog können Einstellungen zur Überwachung von IP-Verbindungen vorgenommen werden, und zwar für die interne LAN Capture-Kontrolle, für das Thread Profiling und für die Heap-Überwachung.

Bereiche

In diesem Dialog gibt es die folgenden Bereiche:

Interne LAN Capture-Kontrolle
Thread-Profiling
Heap-Überwachung

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Übernehmen:* Die geänderten Einstellungen werden gespeichert.
- *Rückgängig:* Die geänderten Einstellungen werden verworfen und auf den Defaultwert zurückgesetzt.

4.7.1.1 Interne LAN Capture-Kontrolle

WBM-Pfad

WBM **>** *Wartung* **>** *Diagnose* **>** *Diagnose-Funktionen* **>** Bereich *Interne LAN Capture-Kontrolle*

Im Bereich *Interne LAN Capture-Kontrolle* können Einstellungen für die interne Überwachung von IP-Paketen im LAN vorgenommen werden. Diese Überwachung erfolgt z. B. mit tshark oder tcpdump. Im Falle eines kritischen Neustarts wird der aktuelle Inhalt in die Backtrace-Datei geschrieben. Beim Starten der Überwachung werden ältere Capture-Dateien gelöscht. Falls diese noch benötigt werden, müssen Sie über *Logs* **>** *Logs exportieren* einen Export durchführen.

Bedienelemente und Anzeigen

Dieser Bereich enthält die folgenden Bedienelemente und Anzeigen:

- Kontrollkästchen:
  - *Nur Headers:* Es sollen nur die Header der IP-Pakete überwacht werden.
  - *Start:* Die interne LAN Capture-Kontrolle soll gestartet werden.
  - *LoopBack-Schnittstelle (nur):* Es soll nur die LoopBack-Schnittstelle benutzt werden.
- Auswahlfeld:
  - *Filter:* Ein Filter zum Überwachen von IP-Paketen kann ausgewählt werden. Auswählbar sind:
    - *kein* (kein Filter)
    - *tcp* (nur IP-Pakete des Transmission Control Protocol)
    - *udp* (nur IP-Pakete des User Datagram Protocol)
- Anzeige:
  - *Status*: Es wird angezeigt, ob die interne LAN Capture-Kontrolle aktiv ist.

4.7.1.2 Thread-Profiling

WBM-Pfad

WBM **>** *Wartung* **>** *Diagnose* **>** *Diagnose-Funktionen* **>** Bereich *Thread-Profiling*

Mit dem Thread Profiling kann überprüft werden, ob Threads die CPU, wie geplant, ausnutzen. D. h. ob ein Thread, von dem man eine niedrige CPU-Belastung erwartet, dies auch wirklich tut.

Bedienelemente und Anzeigen

Dieser Bereich enthält die folgenden Bedienelemente und Anzeigen:

- Kontrollkästchen:
  - *Start:* Das Thread Profiling soll gestartet werden.
- Eingabefelder:

  - *Sample Rate, ms (100-500):* Die Abtastrate kann eingestellt werden, Default ist 250.
  - *Thread-CPU-Nutzung-Grenzwert für Stacktrace, % (10-90):* Es kann eingestellt werden, wie hoch die maximale CPU-Nutzung sein soll, Default ist 50.

- Anzeige:
  - *Status*: Es wird angezeigt, ob das Thread Profiling aktiv ist.

4.7.1.3 Heap-Überwachung

WBM-Pfad

WBM **>** *Wartung* **>** *Diagnose* **>** *Diagnose-Funktionen* **>** Bereich *Heap-Überwachung*

Durch das Erzeugen eines Heap-Dumps können alle Objekte, die sich auf dem Heap befinden, in eine Datei geschrieben werden.

Bedienelemente und Anzeigen

Dieser Bereich enthält die folgenden Bedienelemente und Anzeigen:

- Kontrollkästchen:
  - *Start:* Die Heap-Überwachung soll gestartet werden.
- Eingabefelder:
  - *Sample Rate, ms (500-5000):* Die Abtastrate kann eingestellt werden, Default ist 1000.
  - *Speichergebrauch-Grenzwert für Heapdump, % (50-90):* Es kann eingestellt werden, wieviel Speicher für den Heapdump genutzt werden kann, Default ist 80.
- Anzeige:
  - *Status*: Es wird angezeigt, ob die Heap-Überwachung aktiv ist.

4.7.2 Diagnose-Dateien

WBM-Pfad

WBM **>** *Wartung* **>** *Diagnose* **>** *Diagnose-Dateien*

Der Dialog *Diagnose-Dateien* wird angezeigt.

Auf der RAM-Disk, d.h. einem virtuellen temporären Datenträger im Arbeitsspeicher, werden Protokolldateien abgelegt. Diese Protokolldateien können ausgelesen und in eine Archivdatei gepackt werden. Eine Backtrace-Datei enthält den Inhalt des Stacks im Moment des Erzeugens.

Schaltflächen

In diesem Dialog gibt es die folgenden Schaltflächen:

- *Heap-Dump Erzeugen:* Erzeugt eine Datei, die alle im Moment des Erzeugens erreichbaren Java-Objekte enthält. Anhand dieser Datei lässt sich der Arbeitsspeicherverbrauch analysieren.

HINWEIS: Die Backtrace-Archivdatei (Inhalt der RAMDISK/ramdisk.zip) enthält alle Protokolldateien der RAM-Disk und ist nun beim gewöhnlichen Log-Export enthalten.

4.8 Status-Information

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information*

Das Menü *Status-Information* wird geöffnet.

Menü *Status-Information*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

System-Information
SoftGate-Verbindungskontrolle
H323-Status
HFA WAN Clients

4.8.1 System-Information

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *System-Information*

Das Menü *System-Information* wird geöffnet.

Menü *System-Information*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

Thread Zustände anzeigen
Periphere Baugruppen
OpenScape Access Module
OpenScape Access Clocking
AP Emergency

4.8.1.1 Thread Zustände anzeigen

HINWEIS: Diese Funktion darf nur von Entwicklern benutzt werden.

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *System-Information* **>** *Thread Zustände anzeigen*

Die Tabelle *Thread Zustände* wird angezeigt. In dieser Tabelle werden die gerade aktiven Threads angezeigt. Dazu werden folgende Angaben gemacht:
Thread Name, *Thread ID*, *Hashcode Kontextklasse*, *blockierte Zeit [ms]*, *max. blockierte Zeit [ms]*.

4.8.1.2 Periphere Baugruppen

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *System-Information* **>** *Periphere Baugruppen*

Die Tabelle *Periphere Baugruppen* wird angezeigt. In dieser Tabelle werden die mit OpenScape 4000 SoftGate verbundenen virtuellen peripheren Baugruppen angezeigt. Dazu werden folgende Angaben gemacht:

- *PEN*: Peripheral Equipment Number
- *Typ*: Typ der Baugruppe, hier: virtuelle Baugruppe
- *HW-ID*
- *FCT*
- *Part-Liste*
- *Loadware-Name*
- *Name:* Name der physikalischen peripheren Baugruppe, die virtualisiert wurde
- *Class*

Schaltflächen

In dieser Tabelle gibt es die folgenden Schaltflächen:

Schaltflächen in der Spalte PEN
Schaltflächen detail

Schaltflächen in der Spalte *PEN*

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *System-Information* **>** *Periphere Baugruppen* **>** Schaltfläche in der Spalte *PEN*

Die *Tabelle für Software PEN...* wird angezeigt. In dieser Tabelle werden für die ausgewählte virtuelle periphere Baugruppe folgende Informationen angezeigt: *PEN* (Peripheral Equipment Number), *SubNr.*, *L*, *Status*, *IP-Adresse*, *H225 Port*, *TSA-Status*, *Gesprächs-Ref. ID*, *TSL*, *HWY*, *B-Kanal*.

Schaltfläche

Unter dieser Tabelle gibt es die folgende Schaltfläche:

- *Zurück zu periphere Baugruppen:* Die Tabelle *Periphere Baugruppen* wird wieder angezeigt.

Schaltflächen *detail*

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *System-Information* **>** *Periphere Baugruppen* **>** Schaltfläche *detail*

Die Tabelle *Baugruppen-Details für [PEN]* wird angezeigt (wenn von der Baugruppe unterstützt). In dieser Tabelle werden für die ausgewählte virtuelle periphere Baugruppe folgende Detail-Informationen angezeigt:

- *PEN*: Peripheral Equipment Number
- *PBC*
- *Name*: Name und Sachnummer der physikalischen peripheren Baugruppe, die virtualisiert wurde
- *max. Timeslots: Maximale Anzahl der Zeitschlitze*
- *law*: Digitalisierungsverfahren für analoge Audiosignale (A-law oder µ-law)
- *XLINK MAC-Adresse*: MAC-Adresse des XLink LAN-Interfaces
- *XLINK IP-Adresse*: IP-Adresse des XLink LAN-Interfaces
- *SPA Sachnummer*
- *SPA Kurzname*
- *SPA SW Version*
- *SPA State*
- *LED-RT*: Zustand der roten LED, ein oder aus
- *LED GN*: Zustand der grünen LED, ein oder aus
- *Telco Spannung*
- *Lüfter*: Zustand des Lüfters, in Betrieb oder nicht in Betrieb
- *LAN-FRAMES-OK*: Anzahl der korrekten LAN-Frames für TX (Senden) und RX (Empfangen)
- *LAN-ERRORS*: Anzahl der Fehler für PHY-RX, FCS, SCF und MCF

Schaltfläche

Unter dieser Tabelle gibt es die folgende Schaltfläche:

- *Zurück zu periphere Baugruppen:* Die Tabelle *Periphere Baugruppen* wird wieder angezeigt.

4.8.1.3 OpenScape Access Module

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *System-Information* **>** *OpenScape Access Module*

Die Tabelle *OpenScape Access Module* wird angezeigt. In dieser Tabelle werden die OpenScape Access Module angezeigt. Dazu werden folgende Angaben gemacht:

- *PEN: Peripheral Equipment Number*
- *PBC*
- *LEDs*
- *Status:* in Betrieb oder nicht in Betrieb
- *SPA State*
- *HW-ID*
- *Name*: Name und Sachnummer der physikalischen peripheren Baugruppe, die virtualisiert wurde
- *Class*

Schaltflächen

In dieser Tabelle gibt es die folgenden Schaltflächen:

Schaltflächen in der Spalte PEN
Schaltflächen detail

Schaltflächen in der Spalte *PEN*

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *System-Information* **>** *OpenScape Access Module* **>** *Schaltflächen in der Spalte PEN*

Die *Tabelle für Software PEN...* wird angezeigt. In dieser Tabelle werden für das ausgewählte Access Module Informationen angezeigt.

Schaltfläche

Unter dieser Tabelle gibt es die folgende Schaltfläche:

- *Zurück zu OpenScape Access Module:* Die Tabelle *OpenScape Access Module* wird wieder angezeigt.

Schaltflächen *detail*

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *System-Information* **>** *OpenScape Access Module* **>** *Schaltflächen detail*

Die Tabelle *HPA Modul-Details für [PEN]* wird angezeigt (wenn von der Baugruppe unterstützt). In dieser Tabelle werden für die ausgewählte virtuelle periphere Baugruppe folgende Detail-Informationen angezeigt:

- *PEN*: Peripheral Equipment Number
- *PBC*

- *Name*: Name und Sachnummer der physikalischen peripheren Baugruppe, die virtualisiert wurde
- *max. Timeslots: Maximale Anzahl der Zeitschlitze*
- *law*: Digitalisierungsverfahren für analoge Audiosignale (A-law oder µ-law)
- *XLINK MAC-Adresse*: MAC-Adresse des XLink LAN-Interfaces
- *XLINK IP-Adresse*: IP-Adresse des XLink LAN-Interfaces
- *SPA Sachnummer*
- *SPA Kurzname*
- *SPA SW Version*
- *SPA State*
- *LED-RT*: Zustand der roten LED, ein oder aus
- *LED GN*: Zustand der grünen LED, ein oder aus
- *Telco Spannung*
- *Lüfter*: Zustand des Lüfters, in Betrieb oder nicht in Betrieb
- *LAN-FRAMES-OK*: Anzahl der korrekten LAN-Frames für TX (Senden) und RX (Empfangen)
- *LAN-ERRORS*: Anzahl der Fehler für PHY-RX, FCS, SCF und MCF

Schaltflächen

Unter dieser Tabelle gibt es die folgenden Schaltflächen:

- *Zurück zu OpenScape Access Module:* Die Tabelle *OpenScape Access Module* wird wieder angezeigt.
- *X-LINK RTP Jitter Statistik anfordern*: Die Jitter Statistik für das OpenScape Access Module wird angezeigt.

X-LINK Jitter Statistik für [PEN]

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *System-Information* **>** *OpenScape Access Module* **>** *X-LINK Jitter Statistik für [PEN]*

Die Jitter Statistik für das OpenScape Access Module wird angezeigt.

Schaltfläche

In diesem Dialog gibt es die folgende Schaltfläche:

- *Zurück zu OpenScape Access Module-Details:* Die Tabelle *HPA Modul-Details für [PEN]* wird wieder angezeigt.

4.8.1.4 OpenScape Access Clocking

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *System-Information* **>** *OpenScape Access Clocking*

Die Tabelle *OpenScape Access Clocking* wird angezeigt. In dieser Tabelle werden die Werte für die Taktung der OpenScape Access Module angezeigt. Dazu werden folgende Angaben gemacht:

- *PEN*: Peripheral Equipment Number
- *PBC*
- *Name*: Name und Sachnummer der physikalischen peripheren Baugruppe, die virtualisiert wurde
- *Trunk*
- *SM*
- *CLK-SRC*
- *State*
- *CNT*
- *dF*
- *dP*
- *Sync.Verluste*
- *dP-Avg*
- *VCXO-Center*: Voltage-Controlled Crystal Osczillator
- *VCXO-Avg*: Voltage-Controlled Crystal Osczillator

Schaltflächen

In dieser Tabelle gibt es die folgenden Schaltflächen:

Schaltflächen in der Spalte PEN
Schaltflächen detail

Schaltflächen in der Spalte PEN

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *System-Information* **>** *OpenScape Access Clocking* **>** *Schaltflächen in der Spalte PEN*

In diesem Dialog werden für das ausgewählte Access Module Informationen angezeigt.

Schaltflächen detail

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *System-Information* **>** *OpenScape Access Clocking* **>** *Schaltflächen detail*

Der Dialog *HPA Clocking Details* wird angezeigt. In diesem Dialog werden folgende Grafiken angezeigt:

- *Phase Jitter Distribution*: Verteilung der Phasenschwankungen um einen Mittelwert
- *Phase Jitter*: Phasenschwankungen um einen Mittelwert

Schaltfläche

In diesem Dialog gibt es die folgende Schaltfläche:

- *Zurück zu OpenScape Access Clocking:* Die Tabelle *OpenScape Access Clocking* wird wieder angezeigt.

4.8.1.5 AP Emergency

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *System-Information* **>** *AP Emergency*

Die Tabelle *AP Notfall-Status* wird angezeigt. In dieser Tabelle werden die Daten des AP Emergency dargestellt. Diese Daten sind: *AP*, *Kontrolleinheit*, *Host-CC verbunden*, *CC-AP verbunden*.

AP Emergency übernimmt den Betrieb der Access Points, wenn die zentrale Steuerung ausfällt.

4.8.2 SoftGate-Verbindungskontrolle

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *SoftGate-Verbindungskontrolle*

Das Menü *SoftGate-Verbindungskontrolle* wird geöffnet.

Menü *SoftGate-Verbindungskontrolle*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

IPDA Verbindungen anzeigen
IPDA DMC Verbindungen anzeigen
Alle Verbindungen anzeigen

4.8.2.1 IPDA Verbindungen anzeigen

HINWEIS: Diese Funktion darf nur von Entwicklern benutzt werden.

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *SoftGate-Verbindungskontrolle* **>** *IPDA Verbindungen anzeigen*

Die Tabelle *SCC-N IPDA-Verbindungsliste* wird angezeigt. In dieser Tabelle werden die gerade aktiven IPDA-Verbindungen angezeigt (IPDA: IP Distributed Architecture). Dazu werden folgende Angaben gemacht: *NPCI*, *Teilnehmer A*, *Teilnehmer B*, *SW attr.*, *Codes*, *Ziel-Port*, *Quell-Port*, *IP Adresse*, *Index*.

Schaltfläche

Aktualisieren: Durch Klicken auf diese Schaltfläche wird die Verbindungsliste manuell aktualisiert.

Kontrollkästchen

Autom. Aktualisierung: Aktivierbar/deaktivierbar. Wenn dieses Kontrollkästchen aktiviert ist, wird die Verbindungsliste alle 60 Sekunden automatisch aktualisiert.

Anzeige

Sekunden bis zur nächsten Aktualisierung: Anzeige, in wieviel Sekunden die Verbindungsliste automatisch aktualisiert wird.

4.8.2.2 IPDA DMC Verbindungen anzeigen

HINWEIS: Diese Funktion darf nur von Entwicklern benutzt werden.

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *SoftGate-Verbindungskontrolle* **>** *IPDA DMC Verbindungen anzeigen*

Die Tabelle *SCC-DMC IPDA-Verbindungsliste* wird angezeigt. In dieser Tabelle werden die gerade aktiven IPDA-Verbindungen angezeigt (IPDA: IP Distributed Architecture). Dazu werden folgende Angaben gemacht: *NPCI*, *CorrelationID*, *ForwardCodec*, *ReverseCodec*, *Quell-Port*, *Ziel-Port*, *IP Adresse*.

Schaltfläche

Aktualisieren: Durch Klicken auf diese Schaltfläche wird die Verbindungsliste manuell aktualisiert.

Kontrollkästchen

Autom. Aktualisierung: Aktivierbar/deaktivierbar. Wenn dieses Kontrollkästchen aktiviert ist, wird die Verbindungsliste alle 60 Sekunden automatisch aktualisiert.

Anzeige

Sekunden bis zur nächsten Aktualisierung: Anzeige, in wieviel Sekunden die Verbindungsliste automatisch aktualisiert wird.

4.8.2.3 Alle Verbindungen anzeigen

HINWEIS: Diese Funktion darf nur von Entwicklern benutzt werden.

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *SoftGate-Verbindungskontrolle* **>** *Alle Verbindungen anzeigen*

Die Tabelle *SCC-Verbindungsliste* wird angezeigt. In dieser Tabelle werden alle gerade aktiven SCC-Verbindungen angezeigt. Dazu werden folgende Angaben gemacht: *Baugruppe*, *Typ*.

Schaltfläche

Aktualisieren: Durch Klicken auf diese Schaltfläche wird die Verbindungsliste manuell aktualisiert.

Kontrollkästchen

Autom. Aktualisierung: Aktivierbar/deaktivierbar. Wenn dieses Kontrollkästchen aktiviert ist, wird die Verbindungsliste alle 60 Sekunden automatisch aktualisiert.

Anzeige

Sekunden bis zur nächsten Aktualisierung: Anzeige, in wieviel Sekunden die Verbindungsliste automatisch aktualisiert wird.

4.8.3 H323-Status

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *H323-Status*

Das Menü *H323-Status* wird geöffnet:.

Menü *H323-Status*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

H323 Endpunkte

4.8.3.1 H323 Endpunkte

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *H323-Status* **>** *H323 Endpunkte*

Die Tabelle *H.323 Endpunkte* wird angezeigt. In dieser Tabelle werden die an OpenScape 4000 SoftGate angemeldeten und gerade in Verbindung stehenden H.323-Telefone angezeigt. Dazu werden folgende Angaben gemacht:

- *EP-ID*: Endpunkt-ID
- *Gespräche*: Alle Gespräche am jeweiligen H.323-Endpunkt
- *Ausgehend*: Ausgehende Gespräche am jeweiligen H.323-Endpunkt
- *Ankommend*: Ankommende Gespräche am jeweiligen H.323-Endpunkt
- *Class*

Schaltflächen

In dieser Tabelle gibt es die folgenden Schaltflächen:

Schaltflächen in der Spalte EP-ID
Schaltflächen Details

Schaltflächen in der Spalte *EP-ID*

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *H323-Status* **>** *H323 Endpunkte* **>** Schaltfläche in der Spalte *EP-ID*

Die Tabelle *H.323 Endpunkt...* wird angezeigt.

In dieser Tabelle werden für das ausgewählte H.323-Telefon folgende Informationen angezeigt: *Int. Schlüssel*, *Gesprächs-Ref.*, *Richtung*, *rufender Teilnehmer*, *angerufener Teilnehmer*.

Schaltfläche

Unter dieser Tabelle gibt es die folgende Schaltfläche:

- *Zurück zu H.323 Endpunkteliste*: Die Tabelle *H323 Endpunkt...* wird wieder angezeigt.

Schaltflächen *Details*

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *H323-Status* **>** *H323 Endpunkte* **>** *<Zeile eines H.323-Telefons>* **>** *Details*

Die Tabelle *H.323 Endpunkt Details...* wird angezeigt. Diese Tabelle enthält detaillierte Angaben über das ausgewählte H.323-Telefon. Diese Angaben sind:

- *EP-ID*, *H.323 Produkt ID*, *Nutzer*, *Gesprächsgröße*, *RFC 2198 PT* (Payload for Redundant Audio Data), *RFC 2833 PT* (RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals), *RFC 2833 Ereignisse*
- *Ressourcen*, *ptime*, *maxPtime*, *VAD* (Voice Activity Detection)

Schaltfläche

Unter dieser Tabelle gibt es die folgende Schaltfläche:

- *Zurück zu H.323 Endpunkteliste*: Die Tabelle *H323 Endpunkt Details...* wird wieder angezeigt.

4.8.4 HFA WAN Clients

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *HFA WAN Clients*

Das Menü *HFA WAN Clients* wird geöffnet.

Menü *HFA WAN Clients*

In diesem Menü gibt es die folgenden Auswahlmöglichkeiten:

Status
Logon Versuche

4.8.4.1 Status

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *HFA WAN Clients* **>** *Status*

Die Tabelle *HFA WAN Clients* wird angezeigt. In dieser Tabelle werden für jeden Teilnehmer (HFA WAN Client) folgende Informationen dargestellt: *Teilnehmer*, *Lage*, *Status*, *Adresse*, *Logon um*, *Logoff um*, *Gespräch seit*.

4.8.4.2 Logon Versuche

WBM-Pfad

WBM **>** *Wartung* **>** *Status-Information* **>** *HFA WAN Clients* **>** *Logon Versuche*

Die Tabelle *HFA WAN Clients* wird angezeigt. In dieser Tabelle werden die Teilnehmer (HFA WAN Clients) dargestellt, die vergebliche Logon-Versuche unternommen haben.

4.9 Reboot / Shutdown OS

WBM-Pfad

WBM **>** *Wartung* **>** *Reboot / Shutdown OS*

Das Menü *Reboot / Shutdown OS* wird geöffnet.

Menü *Reboot / Shutdown OS*

In diesem Menü gibt es die folgende Auswahlmöglichkeit:

Reboot / Shutdown OS

4.9.1 Reboot / Shutdown OS

WBM-Pfad

WBM **>** *Wartung* **>** *Reboot / Shutdown OS* **>** *Reboot / Shutdown OS*

Das Fenster *Reboot / Shutdown OS* wird geöffnet. In diesem Fenster kann das Betriebssystem des SoftGates entweder neu gestartet oder heruntergefahren werden.

Schaltflächen

- *Reboot OS*: Durch Klicken auf diese Schaltfläche wird das Betriebssystem des SoftGates heruntergefahren und dann automatisch neu gestartet.
- *Shutdown OS*: Durch Klicken auf diese Schaltfläche wird das Betriebssystem des SoftGates heruntergefahren.

5 Hilfe

Im Modul *Hilfe* werden Informationen über das WBM angezeigt.

WBM-Pfad

WBM **>** *Hilfe*

6 Abmelden

Nach Klicken auf *Abmelden* wird die Verbindung zum OpenScape 4000 SoftGate beendet und die WBM-Sitzung geschlossen.

WBM-Pfad

WBM **>** *Abmelden*

Stichwörter

A
Abmelden 103
Access Clocking 94
Access Module 91
ActiveX 10
Aktion stoppen 60
Aktivitäts-Symbol 16
Alle MEKs entfernen 26
Alle Verbindungen anzeigen 97
Alles 69
Ansagen/MoH (Musik im Wartezustand) 29
Anzahl redundanter Pakete (Parameter) 45
AP Emergency 95
aufeinanderfolgend verarbeitete Pakete (Parameter) 49
aufeinanderfolgend verlorene Pakete (Parameter) 49
Auswahlfelder 17

B
Backtrace-Archiv Erzeugen 88
Backup/Restore 64
Beenden des WBMs 14
Benutzerkennung 13
Benutzername 13
Benutzeroberfläche des WBM 15
Beobachtungszeitraum (s) (Parameter) 48
Berichtsintervall (s) (Parameter) 48

C
ClearMode (ClearChannelData) 45
Clocking 94
Community String 48

D
Datei mit dem Zertifikat (Parameter) 34
Dateidownload 11
Dateigröße des übertragenen Images 60
Diagnose-Dateien 87
Diagnose-Funktionen 85
Dialogelemente 17
DLS Client 79
Dreiecke 18

E
Eingabefelder 17
Einleitung 7
Einstellungen für Picture CLIP 53
Einstellungen für SIP Load Balancer 23
Einstellungen für SPE 35
Entschlüsselungskennwort 33
Export Konfiguration 64
Export Sicherheitskonf. 65
Exportieren
    Logs 68
Externe Ansagen verwalten 29

F
Fax-Kanal mit ermitteltem Ton öffnen 44
Fax-Parameter 44
Fehler-Korrektur-Modus 44
Filter 86
FIPS 140-2 27
FIPS 140-2 Aktivieren 27
FIPS 140-2-Sicherheitsstandard 27

G
Gateway 20
Gateway-Eigenschaften 20
Gateway-Standort 20
Grundeinstellungen 20

H
H323 Endpunkte 98
H323-Status 97
Hard- und Softwarevoraussetzungen 9
Heap-Dump Erzeugen 88
Heap-Überwachung 87
HFA-Interface 41
Hilfe 101

I
Import Konfiguration 65
Import Sicherheitskonf. 66
Informations-Symbol 16
Inhalt dieses Buches 8
Interne Ansagen 30
Interne LAN Capture-Kontrolle 85
Interne MoH Einstellung 30
Internet Explorer 9
IP-Adresse des Network Managements 47
IPDA Verbindungen anzeigen 96

J
Java 10

K

Kennwort 13
Keycert anzeigen 34
Keycert importieren 33
Keycert löschen 35
Konfiguration 19
Konfiguration exportieren 64
Konfiguration importieren 65
Kontrollkästchen 17
Konventionen 8

L

Load Balancer 21
Loadwareaktivierung 59
Loadwareaktualisierung 59
Logs 68
  exportieren 68
  löschen 68
LoopBack-Schnittstelle (nur) 86
LW-Aktivierung 59
LW-Update 59

M

Management Interface Einstellungen 38
Management LAN 38
Master Encryption Key (MEK) Verwaltung 26
Max. UDP-Datagramm-Größe (Byte) 44
Maximaler Netzwerk-Jitter (ms) (Parameter) 45
MEK hinzufügen 26
MEK Verwaltung 26
Menüpunkte 18
Minimale Session-Dauer (* 100 ms) (Parameter) 48
Module 91

N

NCUI 7, 9
NGS Einstellungen 45
Nur Headers 86

O

Oberer Jitter-Schwellwert (ms) (Parameter) 49
OpenScape Access Clocking 94
OpenScape Access Module 91
OpenSSL 27
OpenSSL Verschlüsselungstechnologie 27
OS-Update 61
  Aktionen 62
  Einstellungen 61

P

Passwort 13
PC 9
Periphere Baugruppen 90
Picture CLIP 51, 53
  Direkter Abruf von Bildern 51
  Indirekter Abruf von Bildern 52
Protokolldateien 68
  exportieren 68
  löschen 68
Proxyserver 11

Q

QCU-Empfangsport (Parameter) 47
QCU-IP-Adresse (Parameter) 47
QoS Data Collection 46
Quality of Service Data Collection (QDC) 46

R

Radio-Buttons 17
Rahmengröße 45
Reboot / Shutdown OS 100
Redundantes WAN - Ein/Aus 31
Reset-Symbol 16
Restore 64

S

Sample Rate 87
SCC-Verbindungsliste 96, 97
Schaltflächen 18
Schwellwert für durchschn. Paketlaufzeitverzögerung (ms) (Parameter) 49
Secure Trace 73
  Automatischer Deaktivierungszeitpunkt 76
  Prinzipieller Ablauf 73
  Secure Trace aktiviert 76
  Secure Trace für folgende Protokolle 76
  Status 76
  Trace starten 76
  Trace stoppen 78
  Zertifikat anzeigen 75
  Zertifikat importieren 74
Sende Bericht, wenn (Parameter) 48
Senden an Network Management aktiv (Parameter) 47
Senden an QCU (Parameter) 47
Sicherheit 26
Sicherheitseinstellungen 27
Sicherheitskonfiguration exportieren 65
Sicherheitskonfiguration importieren 66
Signalling Survivability Interface Einstellungen 39
SIP Load Balancer 21
  Einstellungen 23
SIP Load Balancer Status 24
SIP-Interface 42
SoftGate-Verbindungskontrolle 95
Softwarevoraussetzungen 9

Sortierreihenfolge ändern 18
SPE 32
  Einstellungen 35
  Keycert anzeigen 34
  Keycert importieren 33
  Keycert löschen 35
Speichergebrauch-Grenzwert für Heapdump 87
Start 86, 87
Start der Aktion am 60
Start der Aktion in 60
Starten des WBMs 13
Status 76, 86, 87
Status-Information 89
Steuersymbole
  Konzept 16
SW-Update 58
SW-Version anzeigen 58
System Information 89
System-Name 20
Systemzeit 60

T

Telefonbilderzugriff für WAN aktivieren (Picture CLIP) 31
Temporäre Internet-Dateien 10
Thread Zustände anzeigen 89
Thread-CPU-Nutzung-Grenzwert für Stacktrace 87
Thread-Profiling 86
Trace 70
  Profile 70
Trace starten 76
Trace stoppen 78
Trace-Profile-Konfiguration editieren 70

U

Überwachung des LAN 85

V

Verbindungskontrolle 95
verlorene Pakete (pro 1000 Pakete) (Parameter) 49
Verschlüsselungstechnologie
  OpenSSL 27
Version des übertragenen Images 60
Verwendete Fehlerkorrektur (UDP) 44
Voraussetzungen
  Hardware 9
  Software 9

W

WAN 31
WAN Einstellungen 31
WAN Interface - Aktiviert/Deaktiviert 31
Wartung 57
WBM
  beenden 14
  Benutzeroberfläche 15
  Dialog- und Eingabebereich 16
  Dialogelemente 17
  Funktionsbereich 15
  Menübereich 15
  starten 13
  Steuerbereich 16
  Steuersymbole 16
  Symbole 16
Wichtige Hinweise 7
Windows 9

X

XLink 40

Z

Zertifikat anzeigen 75
Zertifikat importieren 74
Zielgruppe 7